Name & Address:
Mark A. Flagel (Bar No. 110635)
355 South Grand Avenue
Los Angeles, California 90071-1560
Telephone: (213) 485-1234
Facsimile: (213) 891-8763

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SYMANTEC CORPORATION and XTREAMLOK, PTY, PLAINTIFF(S) v.	CASE NUMBER **SACV10-01483 JVS (MLGx)**
UNILOC USA, INC., UNILOC (SINGAPORE) PRIVATE LIMITED and UNILOC CORPORATION PTY LIMITED, DEFENDANT(S).	**SUMMONS**

TO: DEFENDANT(S): Uniloc USA, Inc., Uniloc (Singapore) Private Limited, Uniloc Corporation Pty Limited

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached ☑ complaint ☐ _____ amended complaint ☐ counterclaim ☐ cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, Mark A. Flagel, whose address is 355 South Grand Avenue, Los Angeles, California 90071-1560. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Clerk, U.S. District Court

Dated: OCT - 1 2010

By: AMY DeAVILA
Deputy Clerk

(Seal of the Court)

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3)].

LATHAM & WATKINS LLP
Mark A. Flagel (Bar No. 110635)
Yury Kapgan (Bar No. 218366)
Dale Chang (Bar No. 248657)
355 South Grand Avenue
Los Angeles, California 90071-1560
Telephone: (213) 485-1234
Facsimile: (213) 891-8763
mark.flagel@lw.com
yury.kapgan@lw.com
dale.chang@lw.com

LATHAM & WATKINS LLP
Dean G. Dunlavey (Bar No. 115530)
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626-1925
Telephone: (714) 540-1235
Facsimile: (714) 755-8290
dean.dunlavey@lw.com

Attorneys for Plaintiffs
Symantec Corporation and
XtreamLok, Pty

FILED
2010 OCT -1 AM 10:33
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
SANTA ANA
BY:

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SACV10-01483 JVS (MLGx)

SYMANTEC CORPORATION and XTREAMLOK, PTY,

Plaintiffs,

v.

UNILOC USA, INC., UNILOC (SINGAPORE) PRIVATE LIMITED and UNILOC CORPORATION PTY LIMITED,

Defendants.

CIVIL ACTION NO.

COMPLAINT FOR (1) DECLARATORY JUDGMENT AND (2) MONEY PAID TO DEFENDANTS

DEMAND FOR JURY TRIAL

COMPLAINT

Plaintiffs Symantec Corporation ("Symantec") and XtreamLok, Pty ("XtreamLok") hereby plead against Defendants Uniloc USA, Inc., Uniloc (Singapore) Private Limited and Uniloc Corporation Pty Limited (collectively, "Uniloc") the following claims for Declaratory Judgment and Money Paid to Defendants, and allege as follows:

PARTIES

1. Plaintiff Symantec is a Delaware corporation with a principal place of business at 350 Ellis Street, Mountain View, California 94043.

2. Plaintiff XtreamLok is a Proprietary Limited Company existing under the laws of Australia. XtreamLok is an indirect subsidiary of Symantec.

3. On information and belief, Defendant Uniloc USA, Inc. is a corporation with its principal place of business at 2151 Michelson, Suite 100, Irvine, CA 92612, and claims to be the exclusive licensee of U.S. Patent No. 5,490,216 ("the '216 patent"), attached hereto as Exhibit A. In various actions, it has described itself as a Rhode Island corporation and, more recently, a Texas corporation, as described further below, but in all cases it has alleged that its principal place of business is the California address noted above.

4. On information and belief, Defendant Uniloc (Singapore) Private Limited is a limited liability company existing under the laws of Singapore, and owns all right, title and interest in the '216 patent, subject to Uniloc USA, Inc.'s exclusive license.

5. On information and belief, Defendant Uniloc Corporation Pty Limited is a Proprietary Limited Company existing under the laws of Australia. In a 2002 agreement in which Uniloc licensed the '216 patent to XtreamLok, discussed further below, Uniloc Corporation Pty Limited represented that it "is the owner of certain proprietary rights" to the '216 patent.

6. All three Uniloc entities previously filed an action in this Court against Symantec and XtreamLok for infringement of the '216 patent, which was assigned to the Honorable David O. Carter and then stayed pending the resolution of an arbitration, as explained further below.

JURISDICTION AND VENUE

7. The Court has subject matter jurisdiction over this action and the matter pleaded herein under 28 U.S.C. §§ 1331 and 1338(a) because the action arises under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.* and the Patent Act of the United States, 35 U.S.C. § 1, *et seq.* This Court has supplemental jurisdiction over the state law claim alleged herein under 28 U.S.C. § 1367(a).

8. Venue is proper in the United States District Court for the Central District of California pursuant to 28 U.S.C. § 1391(b)(2) in that a substantial part of the acts giving rise to the claim occurred in this District, and all three Uniloc entities, having filed an action in this District and stipulated to continuing jurisdiction within this District, are subject to personal jurisdiction in this District.

GENERAL ALLEGATIONS

9. In May 2008, all three Uniloc entities filed an action in the Central District of California against Symantec and XtreamLok, alleging infringement of the '216 patent, unfair competition and breach of contract (Civil Action No. CV 08-03574 DOC(MLGx)). A copy of the Complaint in that action is attached hereto as Exhibit B. XtreamLok had obtained a license to the '216 patent in a September 2002 agreement, and Uniloc alleged that XtreamLok failed to pay certain royalties owed under the agreement based on revenue that XtreamLok received from its customer, Symantec. Uniloc alleged that XtreamLok breached the agreement, that the agreement was terminated, and that XtreamLok's technology infringed its patent. It also alleged that Symantec was liable for infringement as a result of licensing XtreamLok's technology and thereafter (in

May 2005) indirectly acquiring XtreamLok. Symantec and XtreamLok have consistently maintained that they do not infringe, and that the XtreamLok technology was never covered by, the '216 patent.

10. In October 2008, the parties agreed to arbitrate the breach of contract claim, and to stay the remaining claims pending resolution of that arbitration. Specifically, they stipulated that "once the arbitration of that [breach of contract] claim is concluded, this matter may be re-activated so that this Court may address any remaining claims for Patent Infringement and Unfair Competition." The parties further stipulated that "once the arbitration is concluded, this Court may determine what, if any, impact the decision in the arbitration has on the other claims raised in the Complaint," and that "***this court will retain jurisdiction to decide Uniloc's claims for Patent Infringement*** and Unfair Competition ***to the extent that either party contends any claims or issues remain in accordance with applicable law***." A copy of this Stipulation is attached hereto as Exhibit C. This Court then ordered a stay pending the outcome of the arbitration, specifically noting that it "***shall retain jurisdiction*** over Uniloc's Patent Infringement and Unfair Competition Claims, and shall re-activate the matter upon application of the parties upon completion of the arbitration to allow the continuation of the action as to any claims and issues which either party may contend remain to be resolved in accordance with applicable law." A copy of this Order is attached hereto as Exhibit D.

11. The narrow issue to be addressed in the arbitration was whether, *assuming* (without admitting) that the accused technology was covered by the '216 patent, the 2002 agreement was breached. If the arbitrator determined that there was no breach of contract (with the foregoing assumption), then XtreamLok would have remained licensed to the patent (and Symantec, as XtreamLok's customer, would be protected from liability by the patent exhaustion doctrine). If, on the other hand, the arbitrator determined that there was a breach and

termination of the contract (again, with the foregoing assumption), then the issue of whether XtreamLok and Symantec in fact practiced the '216 patent would be squarely presented to this Court for adjudication. The parties stipulated that the arbitration would not cover or address the issue of whether the technology was in fact covered by the '216 patent, with that question being reserved exclusively for Judge Carter's court. The parties further stipulated that this Court would retain jurisdiction to resolve the infringement and other issues after the conclusion of the arbitration.

12. In September 2009, the arbitrator issued her ruling, expressly noted that no ruling was rendered on the substantive issue of whether the XtreamLok technology practiced the patent, and held that, in light of the parties' stipulated arbitration assumption, royalties had been underpaid and, as a result, the contract had been breached and terminated. She ordered XtreamLok to pay the Uniloc entities the amount she calculated as the underpayment, with interest. XtreamLok did in fact pay this award to Uniloc. The payment, however, was subject to the express reservation by XtreamLok of the right to seek return of the money, because that money would never have been due and owing to Uniloc if (and thus was not owing to Uniloc because), as XtreamLok and Symantec have always contended, the XtreamLok technology is not covered by the '216 patent.

13. After the arbitration concluded, rather than return to this Court to have the remaining issues resolved, on November 30, 2009, Uniloc unilaterally dismissed the then-pending action, under Federal Rule of Civil Procedure 41(a). Simultaneously, Uniloc filed an action for infringement of the '216 patent against other defendants in the Eastern District of Texas. In fact, since dismissing the lawsuit in this Court, Uniloc initiated no fewer than six lawsuits against at least 77 defendants in the Eastern District of Texas, alleging infringement of the '216 patent.

14. In its latest Texas lawsuit filed on September 14, 2010 (Civil Action No. 6:10-CV-472), Uniloc sued Symantec again for infringement of the same patent, despite the parties' earlier Stipulation and this Court's Order. After having voluntarily submitted to (and, indeed, affirmatively invoked) this Court's jurisdiction, and after stipulating that its infringement claim against Symantec would be decided in Judge Carter's court in this District (and where its headquarters are located), Uniloc simply tried to do an end run around this Court in favor of a different forum with little connection to either party.

15. Uniloc's allegations in the Texas actions are revealing. In the first three of the Texas actions, Uniloc USA, Inc. (the purported exclusive licensee of the '216 patent) alleges that it is a Rhode Island corporation, as it had alleged in this Court in its 2008 action against Symantec and XtreamLok. In the next three actions, including the one against Symantec, Uniloc USA alleges instead that it is a Texas corporation. In all actions, however, Uniloc USA admits that its principal place of business is in Irvine, California. On information and belief, the Texas corporation was formed in July 2010, only weeks before Uniloc sued Symantec.

16. Symantec and XtreamLok file this action to finish what Uniloc started in this forum. Symantec and XtreamLok deny that any of their products infringe or have ever infringed any claim of the '216 patent, and also deny that the '216 patent is valid. Because it does not and has never practiced the '216 patent, and because the patent is invalid in any event, XtreamLok also seeks the return of the money paid to Uniloc in connection with the arbitration, which must be returned upon a finding that, contrary to the assumption utilized in the arbitration, no valid claim of the '216 patent is or was infringed by the XtreamLok technology.

FIRST CLAIM FOR RELIEF

(By Symantec and XtreamLok Against All Defendants)

Declaratory Relief Regarding Non-Infringement

17. Symantec and XtreamLok incorporate herein the allegations of paragraphs 1-16.

18. An actual and justiciable controversy exists between Symantec and XtreamLok on the one hand, and Uniloc on the other, as to the non-infringement of the '216 patent.

19. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, Symantec and XtreamLok request a declaration of the Court that they do not infringe and have not infringed any claim of the '216 patent.

SECOND CLAIM FOR RELIEF

(By Symantec and XtreamLok Against All Defendants)

Declaratory Relief Regarding Invalidity

20. Symantec and XtreamLok incorporate herein the allegations of paragraphs 1-19.

21. An actual and justiciable controversy exists between Symantec and XtreamLok, on the one hand, and Uniloc on the other, as to the invalidity of the '216 patent.

22. Pursuant to the Federal Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.*, Symantec and XtreamLok request a declaration of the Court that the '216 patent is invalid under the Patent Act, 35 U.S.C. §§ 41 *et seq.*, including but not limited to sections 101, 102, 103, and 112.

THIRD CLAIM FOR RELIEF

(By XtreamLok Against All Defendants)

Money Paid to Defendants (Common Law)

23. XtreamLok incorporates herein the allegations of paragraphs 1-22.

24. Pursuant to an award by the arbitrator, XtreamLok paid to Uniloc royalties allegedly owed under a 2002 agreement, subject to the express condition that the payment would be returned to XtreamLok were this Court to later determine that the XtreamLok technology did not infringe any valid claim of the '216 patent.

25. Because XtreamLok does not and has never practiced the '216 patent, and because the patent is invalid in any event, XtreamLok is entitled to a return of the money that it paid to Uniloc pursuant to the arbitrator's award, together with interest as appropriate from the time the payment was made until the time that it is returned.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Symantec respectfully requests that the Court enter declaratory judgment as follows:

1. That Symantec does not infringe and has not infringed, directly or indirectly, the '216 patent;

2. That the '216 patent is invalid;

3. That Uniloc, and all persons acting on its behalf or in concert with it, be permanently enjoined and restrained from charging, orally or in writing, that the '216 patent is infringed by Symantec, directly or indirectly;

4. That Symantec be awarded its costs, expenses and reasonable attorney fees in this action; and

5. That Symantec be awarded such other and further relief as the Court may deem appropriate.

WHEREFORE, Plaintiff XtreamLok respectfully requests that the Court enter judgment as follows:

1. That XtreamLok does not infringe and has not infringed, directly or indirectly, the '216 patent;

2. That the '216 patent is invalid;

3. That Uniloc, and all persons acting on its behalf or in concert with it, be permanently enjoined and restrained from charging, orally or in writing, that the '216 patent is infringed by XtreamLok, directly or indirectly;

4. That Uniloc return forthwith to XtreamLok the money that XtreamLok paid to Uniloc pursuant to the arbitrator's conditional award, plus interest;

5. That XtreamLok be awarded its costs, expenses and reasonable attorney fees in this action; and

6. That XtreamLok be awarded such other and further relief as the Court may deem appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully demand a jury trial in this action, as to all issues so triable.

Dated: October 1, 2010

LATHAM & WATKINS LLP

By _____
Mark A. Flagel
Attorneys for Plaintiffs
SYMANTEC CORPORATION AND
XTREAMLOK, PTY

EXHIBIT A

US005490216A

United States Patent [19]

Richardson, III

[11] Patent Number: 5,490,216

[45] Date of Patent: Feb. 6, 1996

[54] **SYSTEM FOR SOFTWARE REGISTRATION**

[75] Inventor: **Frederic B. Richardson, III**, Brookvale, Australia

[73] Assignee: **Uniloc Private Limited**, Singapore

[21] Appl. No.: **124,718**

[22] Filed: **Sep. 21, 1993**

[30] **Foreign Application Priority Data**

Sep. 21, 1992 [AU] Australia PL4842
Oct. 26, 1992 [AU] Australia PL5524

[51] **Int. Cl.**[6] **H04L 9/00**
[52] **U.S. Cl.** **380/4**; 380/23
[58] **Field of Search** 380/3, 4, 23, 24, 380/25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,654,799	3/1987	Ogaki et al.	
4,688,169	8/1987	Joshi .	
4,796,220	1/1989	Wolfe .	
4,982,430	1/1991	Frezza et al. .	
4,999,806	3/1991	Chernow et al.	380/4
5,191,611	3/1993	Lang	380/4
5,199,066	3/1993	Logan	380/4
5,222,133	6/1993	Chou et al.	380/4
5,239,166	8/1993	Graves .	
5,239,648	8/1993	Nukui	380/4
5,287,408	2/1994	Samson	380/4
5,291,598	3/1994	Grundy .	
5,313,637	5/1994	Rose	380/4
5,319,705	7/1994	Halter et al.	380/4
5,337,357	8/1994	Chou et al.	380/4
5,343,526	8/1994	Lassers	380/4
5,349,643	9/1994	Cox et al.	380/4
5,371,792	12/1994	Asai et al.	380/4
5,379,433	1/1995	Yamagishi	380/4
5,386,468	1/1995	Akiyama et al.	380/4
5,388,211	2/1995	Hombuckle	380/4
5,390,297	2/1995	Barber et al.	380/4

FOREIGN PATENT DOCUMENTS

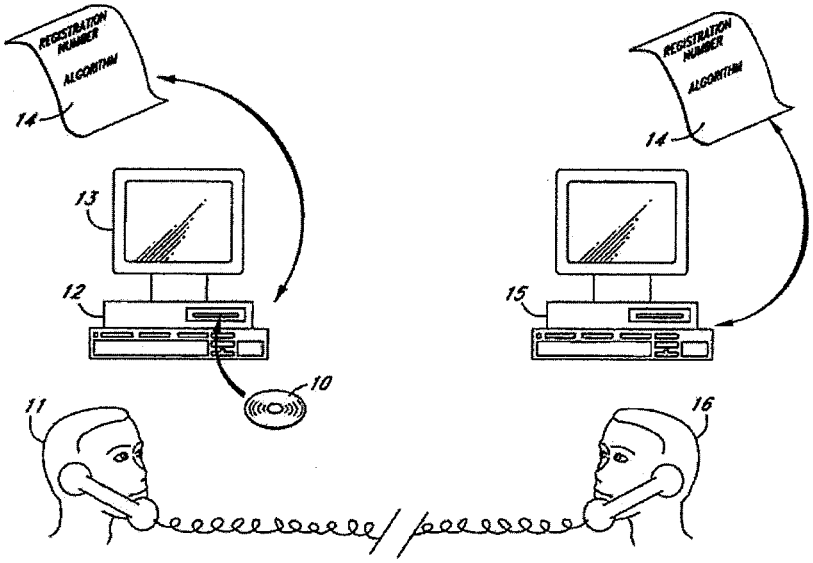
WO9209160 5/1992 WIPO .

Primary Examiner—David C. Cain
Attorney, Agent, or Firm—Knobbe, Martens, Olson & Bear

[57] **ABSTRACT**

A registration system allows digital data or software to run in a use mode on a platform if and only if an appropriate licensing procedure has been followed. Preferably, the system detects when part of the platform on which the digital data has been loaded has changed in part or in entirety, as compared with the platform parameters, when the software or digital data to be protected was last booted or run. The system relies on a portion of digital data or code which is integral to the digital data to be protected by the system. This integral portion is termed the code portion and may include an algorithm that generates a registration number unique to an intending licensee of the digital data based on information supplied by the licensee which characterizes the licensee. The algorithm in the code portion is duplicated at a remote location on a platform under the control of the licensor or its agents, and communication between the intending licensee and the licensor or its agent is required so that a matching registration number can be generated at the remote location for subsequent communication to the intending licensee as a permit to licensed operation of the digital data in a use mode. The code portion can be identical for all copies of the digital data. The algorithm provides a registration number which can be "unique" if the details provided by the intending licenses upon which the algorithm relies when executed upon the platform are themselves "unique".

20 Claims, 12 Drawing Sheets



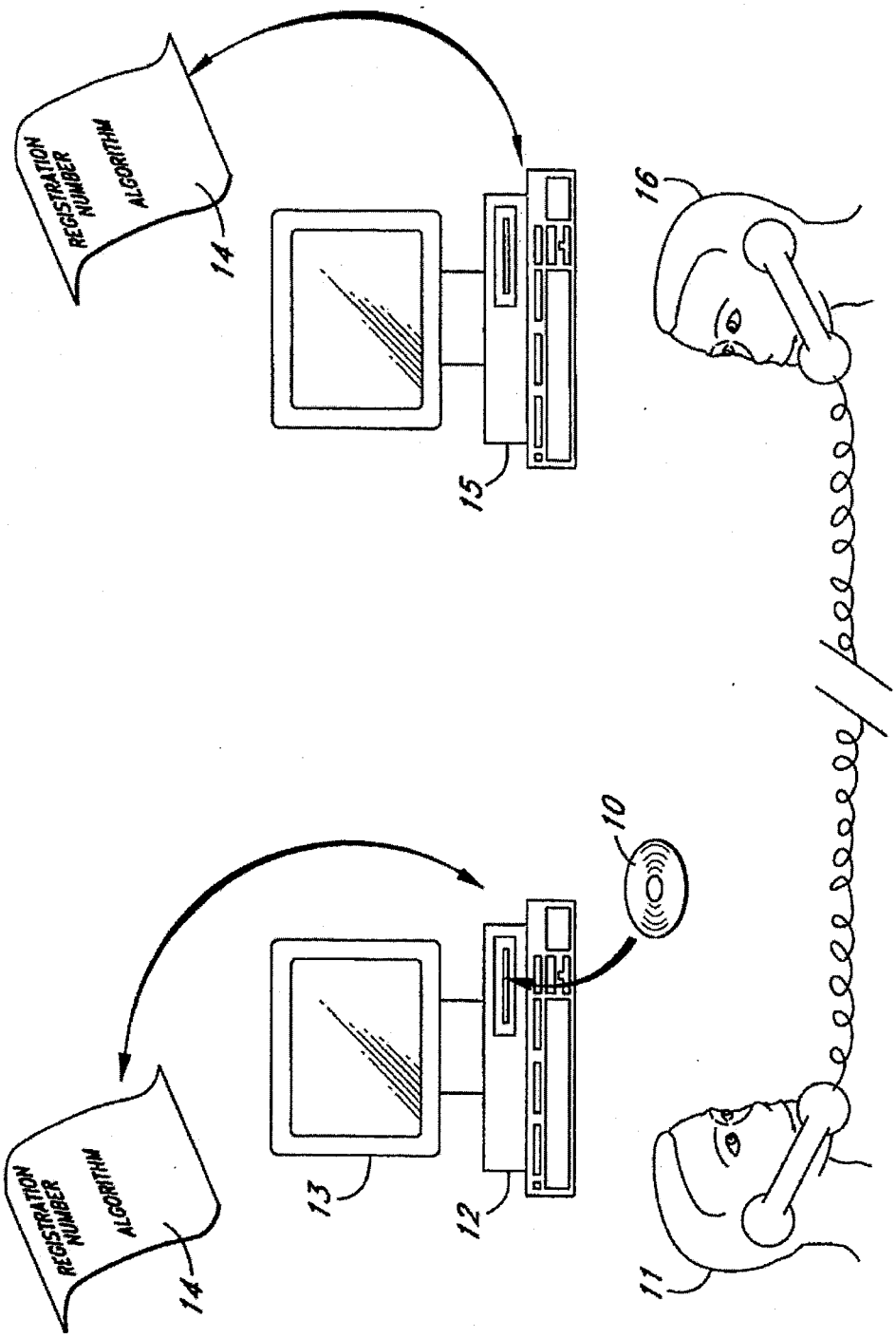


FIG. 1

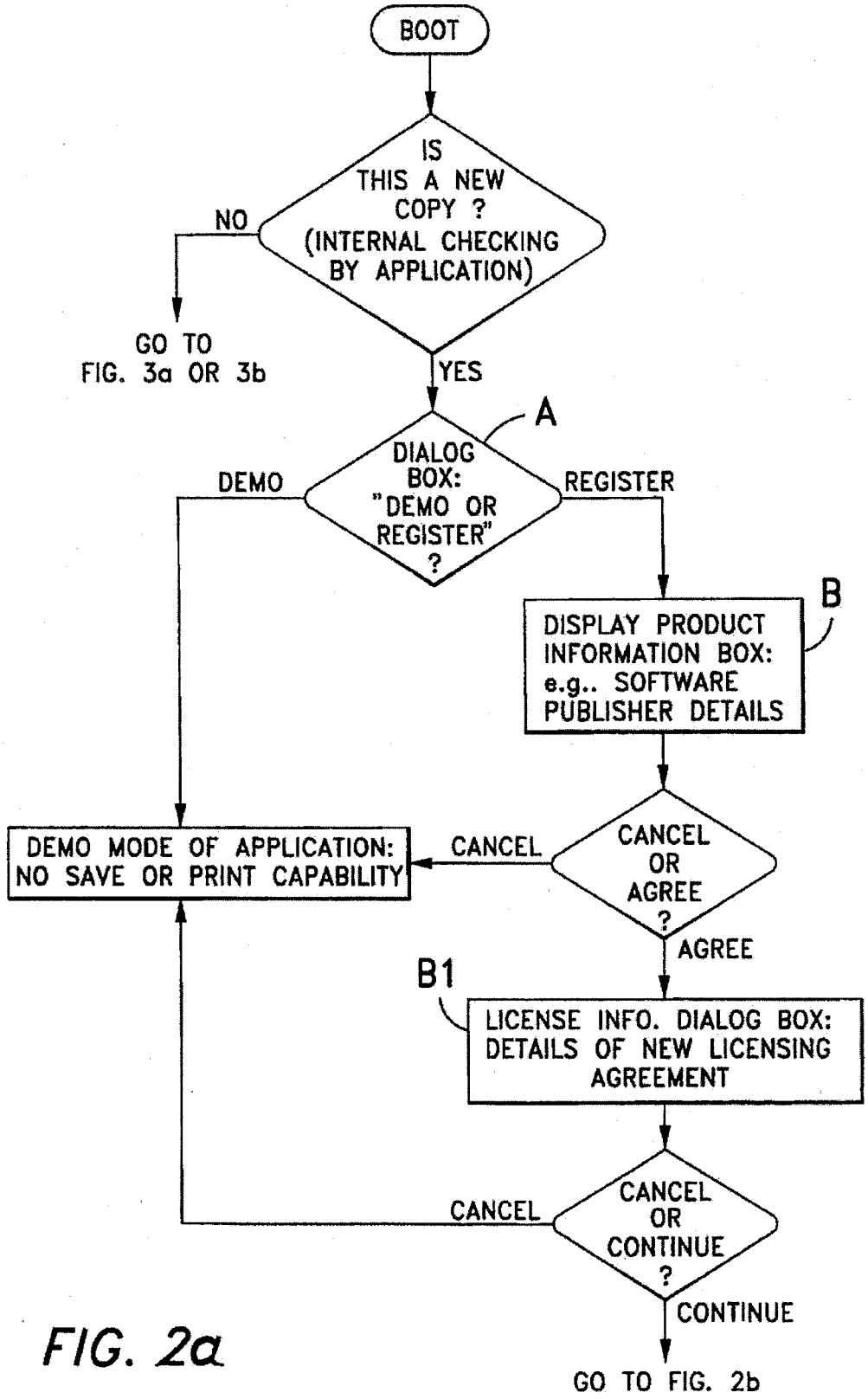

BOOT
IS THIS A NEW COPY ? (INTERNAL CHECKING BY APPLICATION)
NO
GO TO FIG. 3a OR 3b
YES
A
DIALOG BOX: "DEMO OR REGISTER" ?
DEMO
REGISTER
B
DISPLAY PRODUCT INFORMATION BOX: e.g.. SOFTWARE PUBLISHER DETAILS
CANCEL OR AGREE ?
CANCEL
DEMO MODE OF APPLICATION: NO SAVE OR PRINT CAPABILITY
AGREE
B1
LICENSE INFO. DIALOG BOX: DETAILS OF NEW LICENSING AGREEMENT
CANCEL OR CONTINUE ?
CANCEL
CONTINUE
GO TO FIG. 2b

FIG. 2a

FIG. 2b

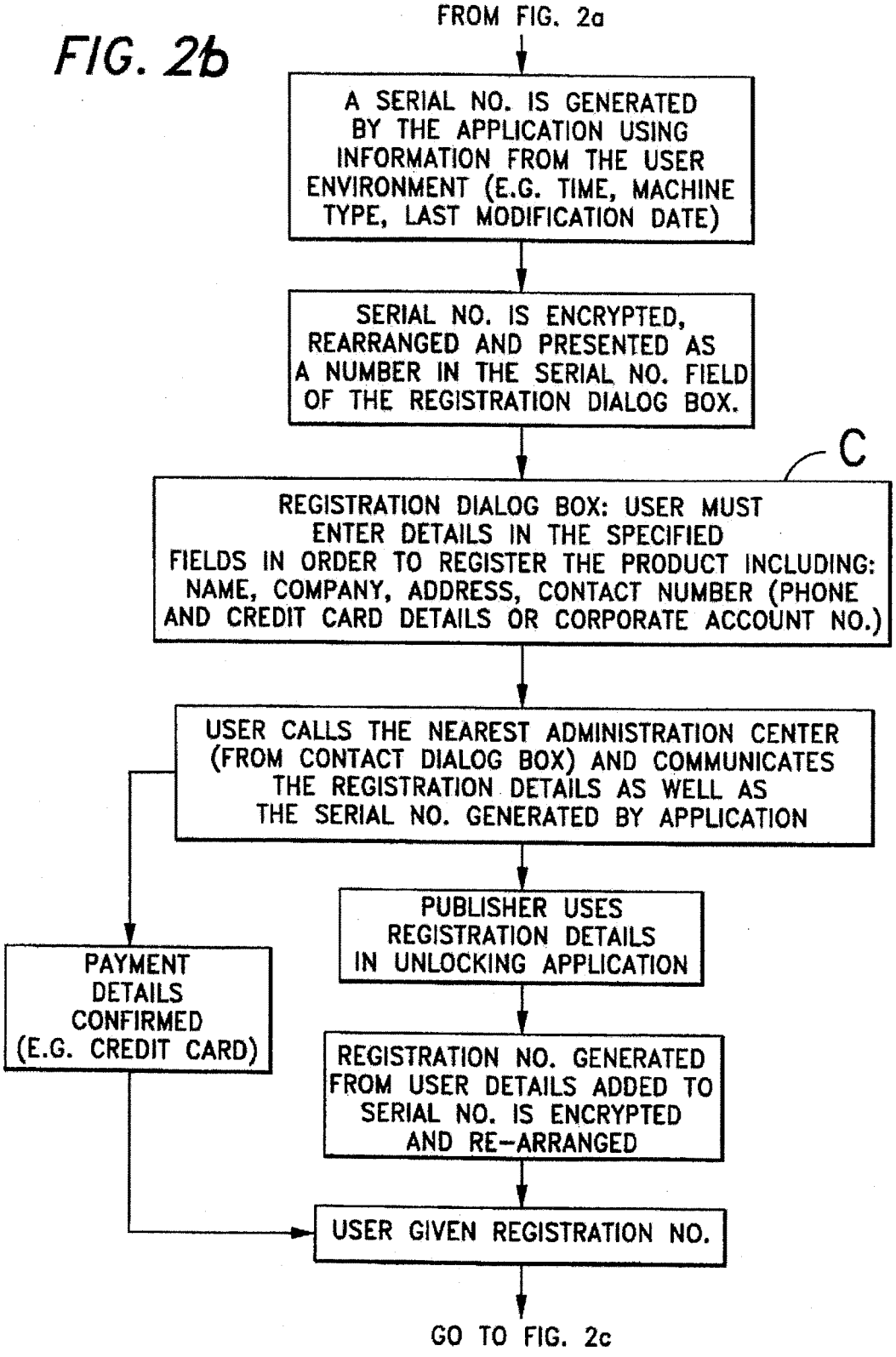

FROM FIG. 2a
A SERIAL NO. IS GENERATED BY THE APPLICATION USING INFORMATION FROM THE USER ENVIRONMENT (E.G. TIME, MACHINE TYPE, LAST MODIFICATION DATE)
SERIAL NO. IS ENCRYPTED, REARRANGED AND PRESENTED AS A NUMBER IN THE SERIAL NO. FIELD OF THE REGISTRATION DIALOG BOX.
C
REGISTRATION DIALOG BOX: USER MUST ENTER DETAILS IN THE SPECIFIED FIELDS IN ORDER TO REGISTER THE PRODUCT INCLUDING: NAME, COMPANY, ADDRESS, CONTACT NUMBER (PHONE AND CREDIT CARD DETAILS OR CORPORATE ACCOUNT NO.)
USER CALLS THE NEAREST ADMINISTRATION CENTER (FROM CONTACT DIALOG BOX) AND COMMUNICATES THE REGISTRATION DETAILS AS WELL AS THE SERIAL NO. GENERATED BY APPLICATION
PUBLISHER USES REGISTRATION DETAILS IN UNLOCKING APPLICATION
PAYMENT DETAILS CONFIRMED (E.G. CREDIT CARD)
REGISTRATION NO. GENERATED FROM USER DETAILS ADDED TO SERIAL NO. IS ENCRYPTED AND RE-ARRANGED
USER GIVEN REGISTRATION NO.
GO TO FIG. 2c

FIG. 2c

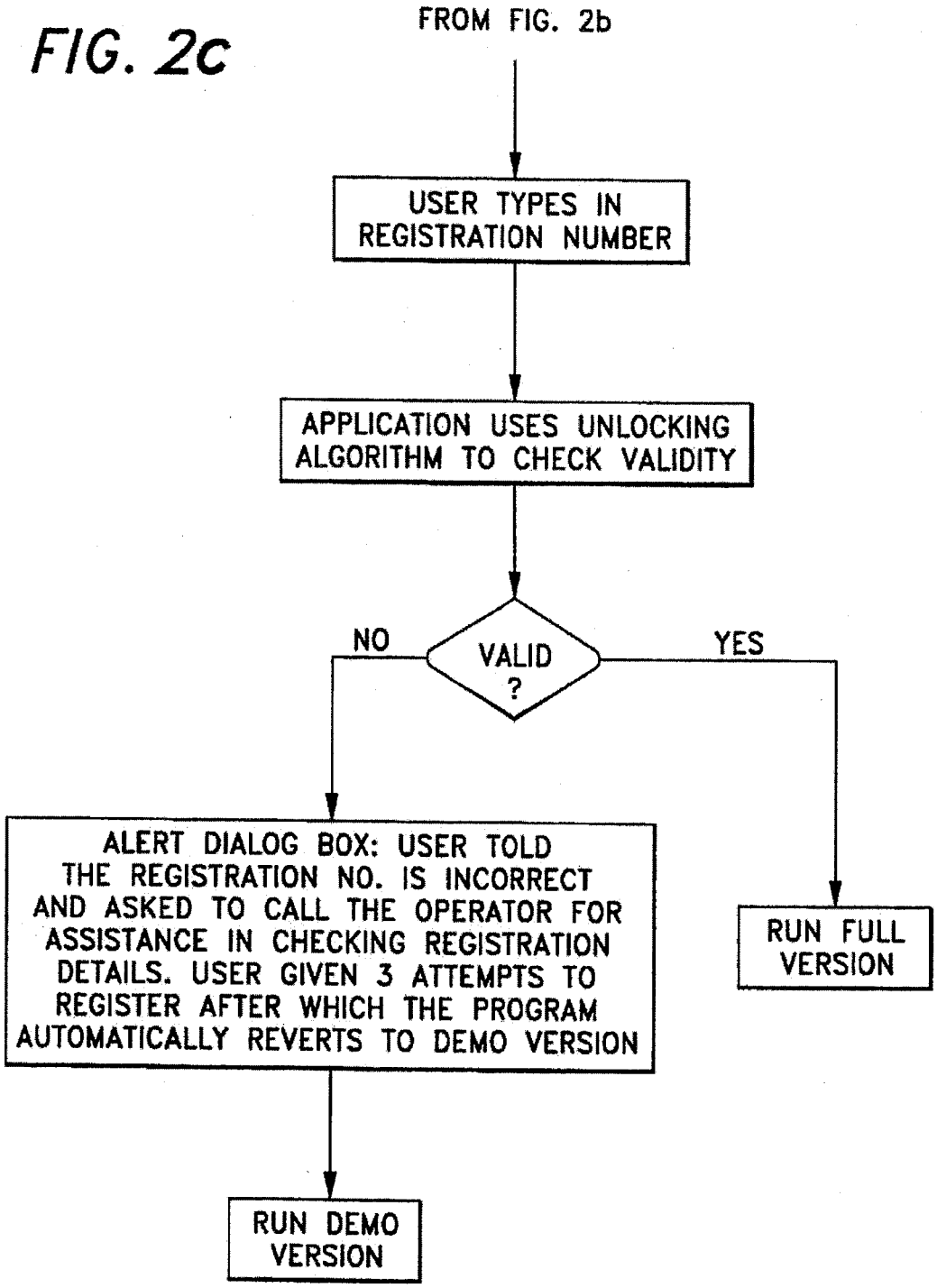
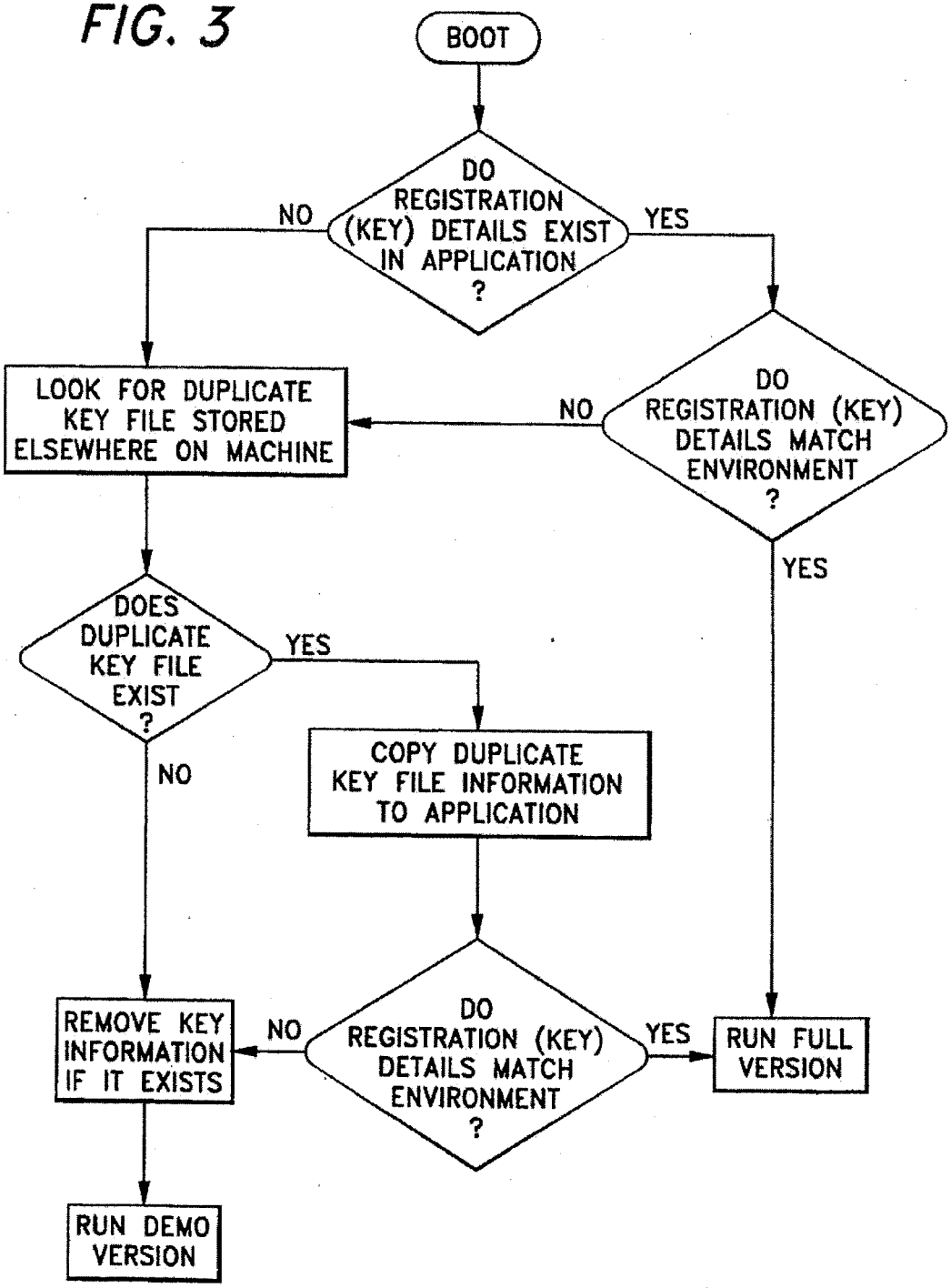

FROM FIG. 2b
USER TYPES IN REGISTRATION NUMBER
APPLICATION USES UNLOCKING ALGORITHM TO CHECK VALIDITY
VALID ?
NO
YES
ALERT DIALOG BOX: USER TOLD THE REGISTRATION NO. IS INCORRECT AND ASKED TO CALL THE OPERATOR FOR ASSISTANCE IN CHECKING REGISTRATION DETAILS. USER GIVEN 3 ATTEMPTS TO REGISTER AFTER WHICH THE PROGRAM AUTOMATICALLY REVERTS TO DEMO VERSION
RUN FULL VERSION
RUN DEMO VERSION

FIG. 3


BOOT
DO REGISTRATION (KEY) DETAILS EXIST IN APPLICATION ?
NO
YES
LOOK FOR DUPLICATE KEY FILE STORED ELSEWHERE ON MACHINE
NO
DO REGISTRATION (KEY) DETAILS MATCH ENVIRONMENT ?
YES
DOES DUPLICATE KEY FILE EXIST ?
YES
NO
COPY DUPLICATE KEY FILE INFORMATION TO APPLICATION
REMOVE KEY INFORMATION IF IT EXISTS
NO
DO REGISTRATION (KEY) DETAILS MATCH ENVIRONMENT ?
YES
RUN FULL VERSION
RUN DEMO VERSION

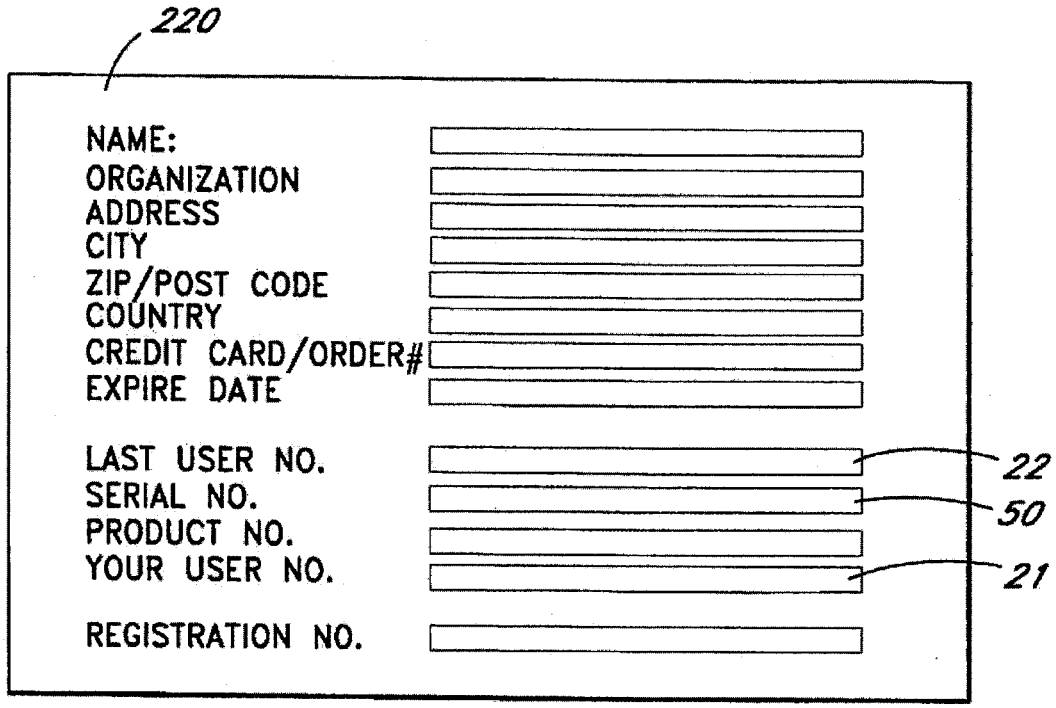

220
NAME:
ORGANIZATION
ADDRESS
CITY
ZIP/POST CODE
COUNTRY
CREDIT CARD/ORDER#
EXPIRE DATE
LAST USER NO.
SERIAL NO.
PRODUCT NO.
YOUR USER NO.
REGISTRATION NO.
22
50
21

FIG. 4

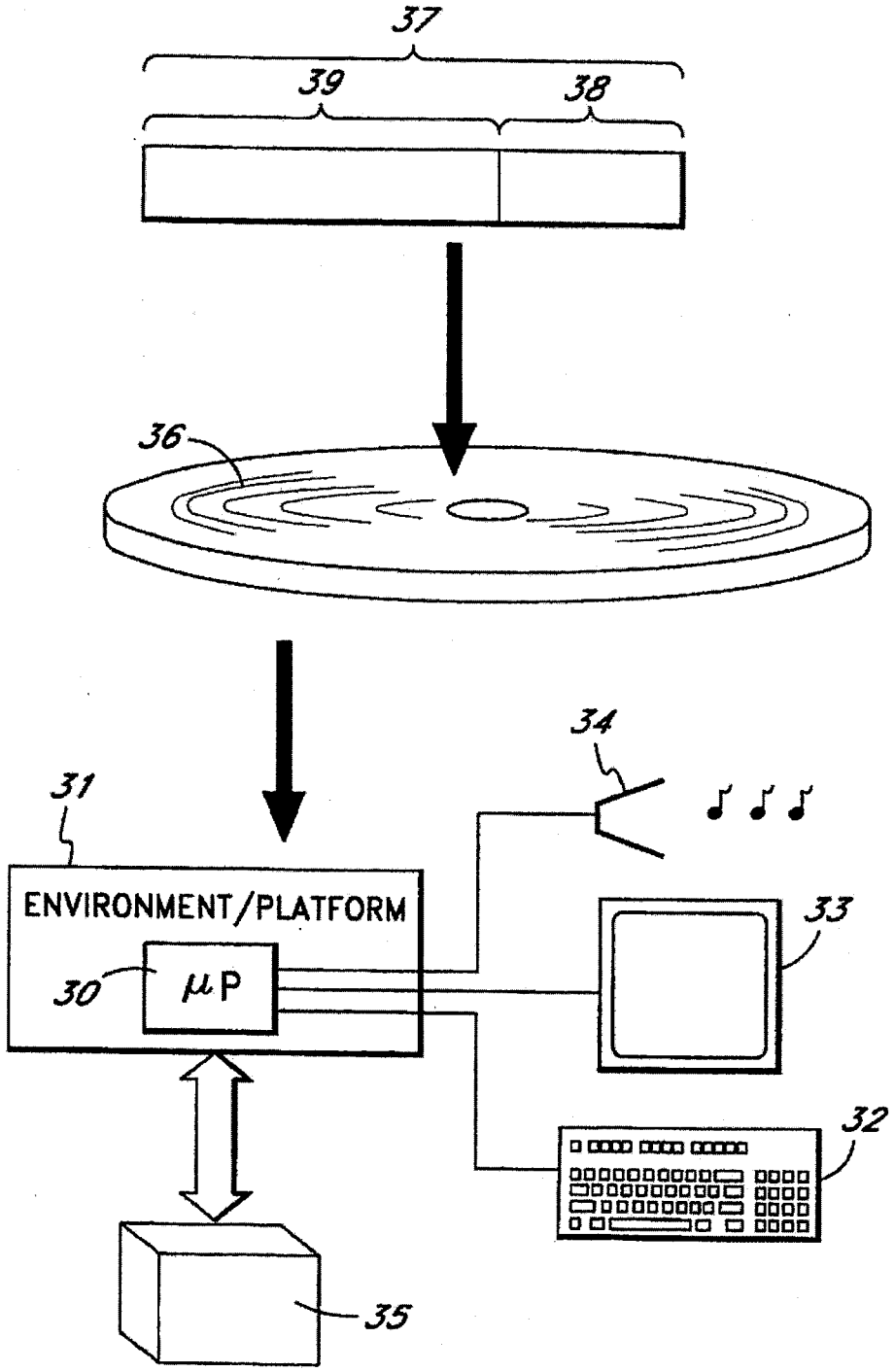


FIG. 5

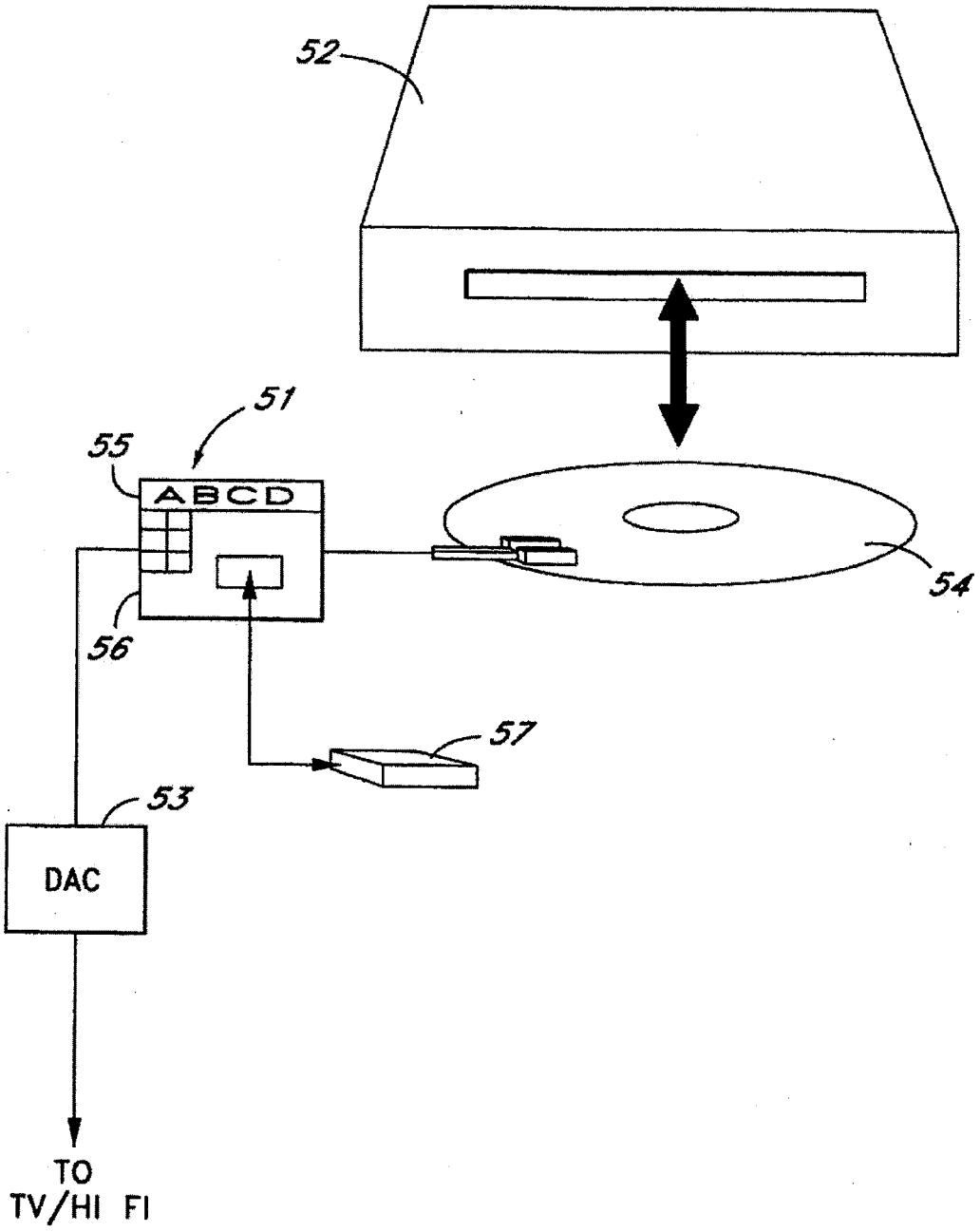


FIG. 6

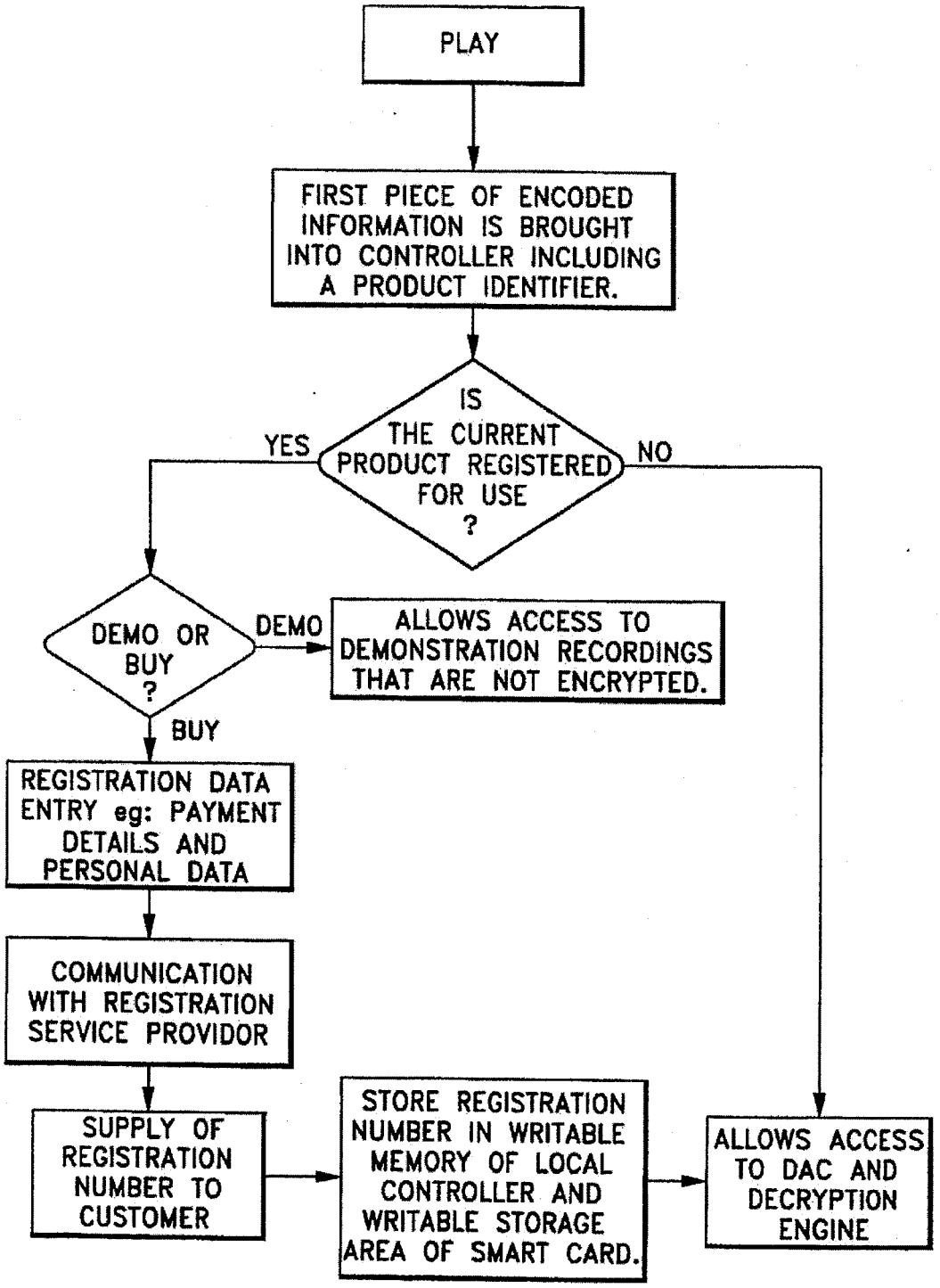

PLAY
FIRST PIECE OF ENCODED INFORMATION IS BROUGHT INTO CONTROLLER INCLUDING A PRODUCT IDENTIFIER.
IS THE CURRENT PRODUCT REGISTERED FOR USE ?
YES
NO
DEMO OR BUY ?
DEMO
ALLOWS ACCESS TO DEMONSTRATION RECORDINGS THAT ARE NOT ENCRYPTED.
BUY
REGISTRATION DATA ENTRY eg: PAYMENT DETAILS AND PERSONAL DATA
COMMUNICATION WITH REGISTRATION SERVICE PROVIDOR
SUPPLY OF REGISTRATION NUMBER TO CUSTOMER
STORE REGISTRATION NUMBER IN WRITABLE MEMORY OF LOCAL CONTROLLER AND WRITABLE STORAGE AREA OF SMART CARD.
ALLOWS ACCESS TO DAC AND DECRYPTION ENGINE

FIG. 7

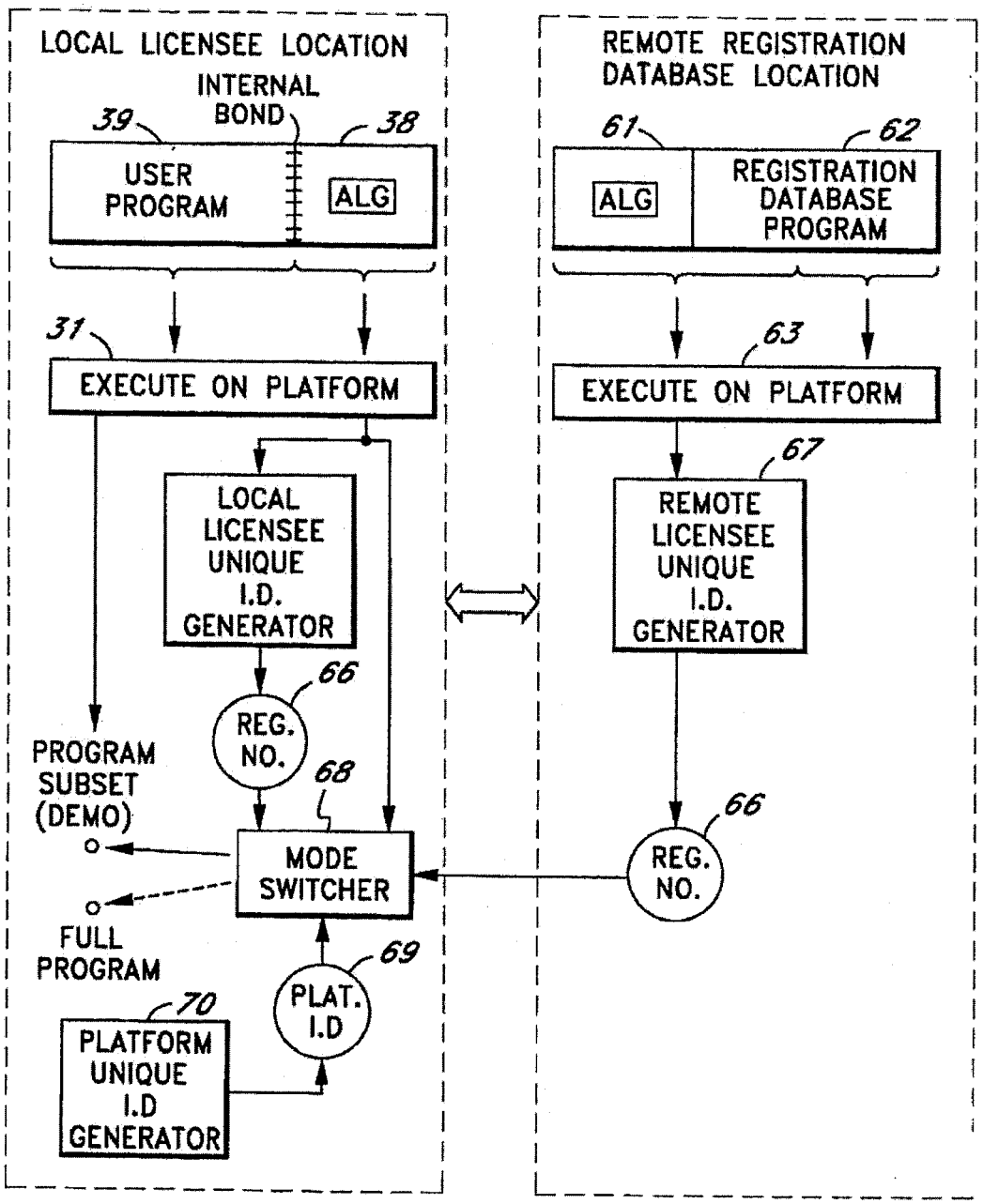

LOCAL LICENSEE LOCATION
INTERNAL BOND
39
38
USER PROGRAM
ALG
31
EXECUTE ON PLATFORM
LOCAL LICENSEE UNIQUE I.D. GENERATOR
66
REG. NO.
PROGRAM SUBSET (DEMO)
68
MODE SWITCHER
FULL PROGRAM
69
PLAT. I.D
70
PLATFORM UNIQUE I.D GENERATOR
REMOTE REGISTRATION DATABASE LOCATION
61
62
ALG
REGISTRATION DATABASE PROGRAM
63
EXECUTE ON PLATFORM
67
REMOTE LICENSEE UNIQUE I.D. GENERATOR
66
REG. NO.

FIG. 8

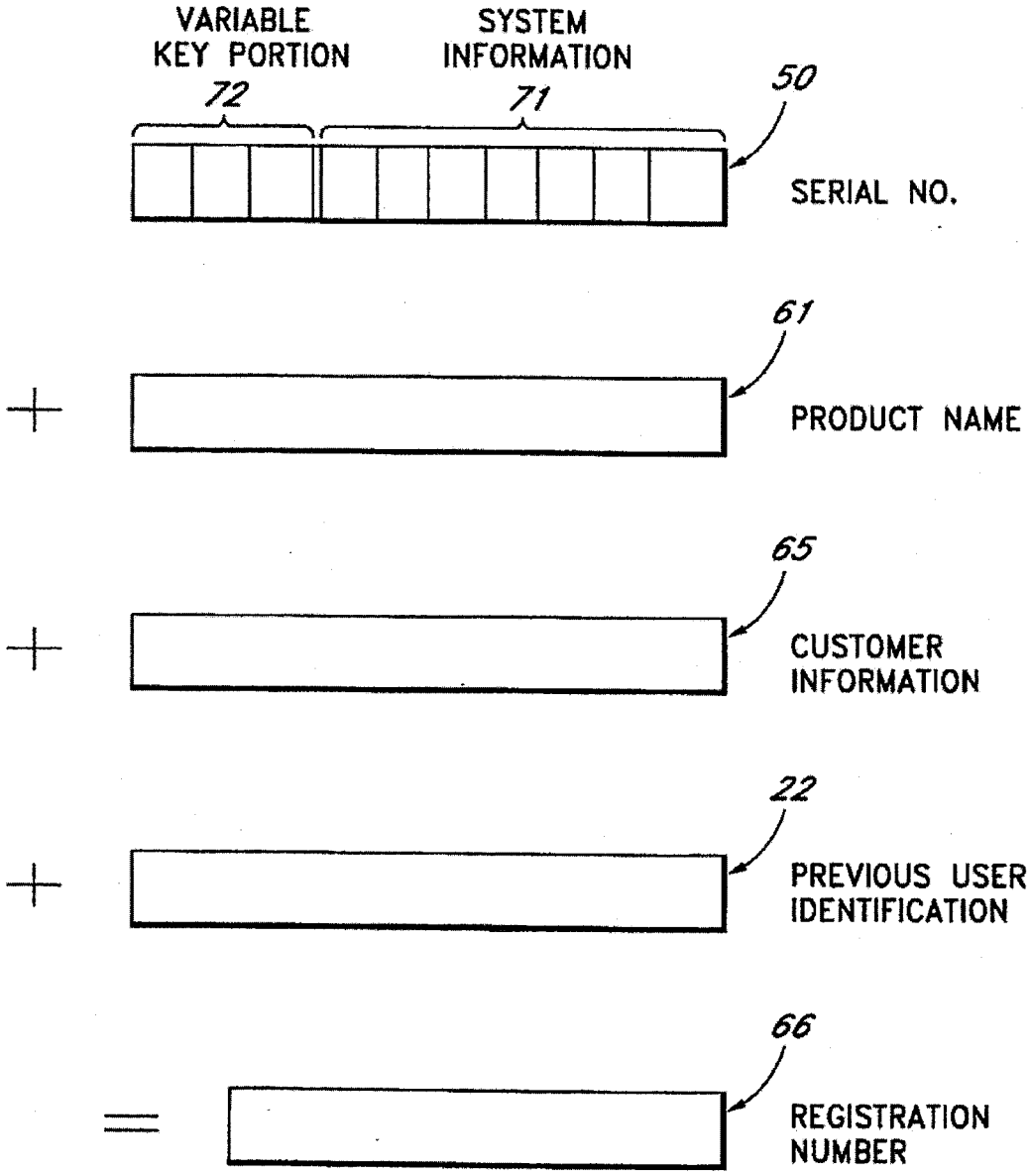

VARIABLE KEY PORTION
72
SYSTEM INFORMATION
71
50
SERIAL NO.
61
PRODUCT NAME
65
CUSTOMER INFORMATION
22
PREVIOUS USER IDENTIFICATION
66
REGISTRATION NUMBER

FIG. 9

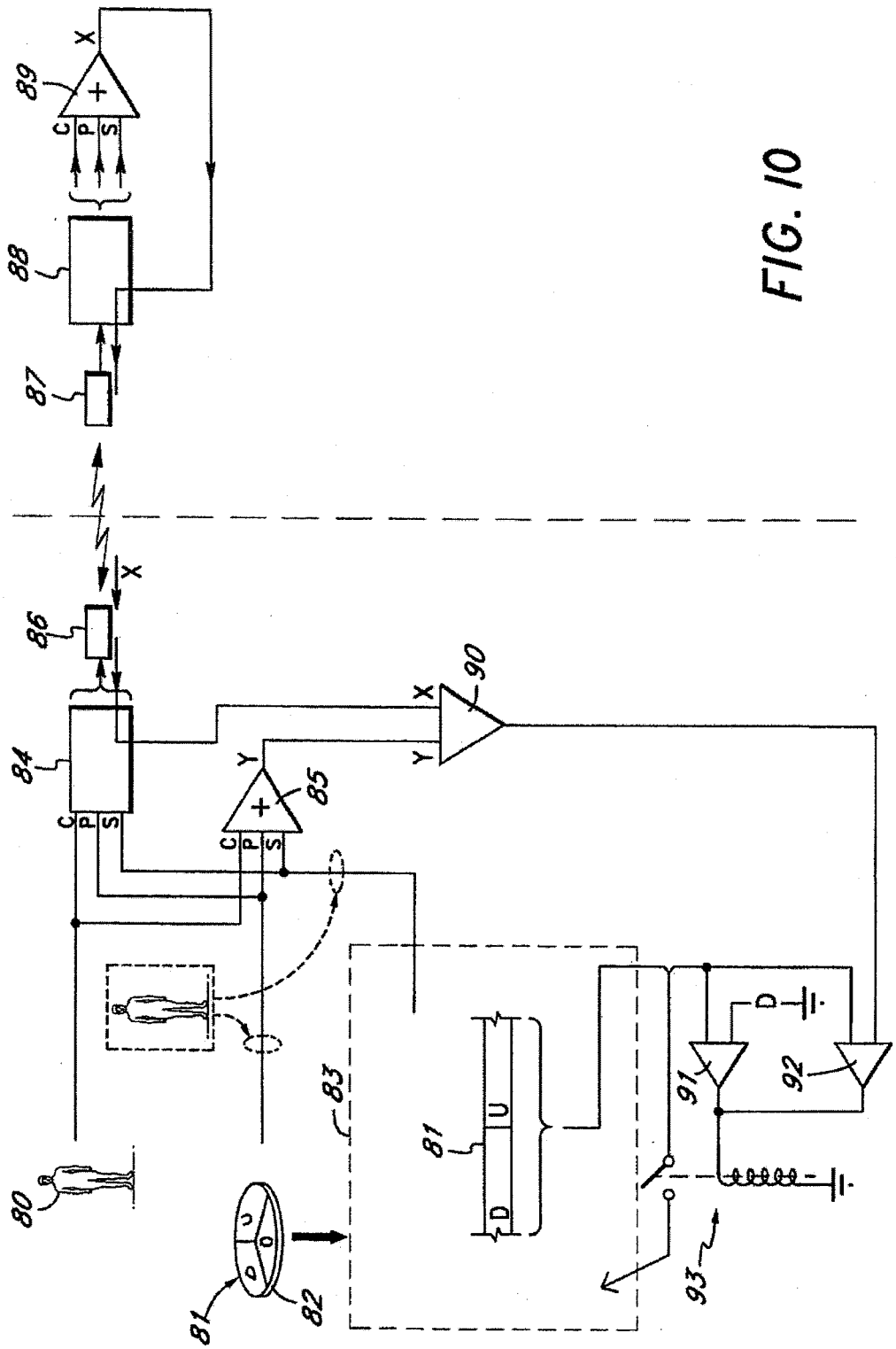


FIG. 10

SYSTEM FOR SOFTWARE REGISTRATION

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to improvements in systems for software registration and, more particularly, to improvements in arrangements where software is transferable by media such as magnetic disks, CD ROMS and the like.

2. Description of the Related Art

Much commercially available software is provided at time of purchase (or license) on a magnetic media, typically a floppy disk. Frequently the only security feature attached to the software is a simple registration number stored on the media. This registration number identifies that particular copy of the software and it is often required at the time of installation of the software onto any given computer that the installer must provide the registration number independently to the installation routines.

However, such simple security arrangements for the distribution of software on media suffer from at lest two disadvantages: (1) each copy of the software made on any given media at the time of manufacture must include an individual, unique number, programmed into the media, and (2) this arrangement does not prevent copying of the software, once installed on any given computer, to another computer by means of file transfer (as opposed to reinstallation).

WO 92/09,160 to Tan Systems Corporation discloses a registration system which is relatively sophisticated which relies for its security on a requirement that an intending software licensee must obtain from a remote location by file transfer significant and essential portions of the program which the licensee desires to execute. The arrangement disclosed in WO 92/09,160 suffers from a number of deficiencies including:

a. the shell program which the intending licensee initially executes requires a unique identity embodied within the shell prior to distribution of the shell program;

b. the shell program is not, itself, a functional program—that is, it does not include all of the code which the intending licensee wishes to execute. That program must be obtained remotely with all the delays, inconveniences and possibilities of corruption during transit that that entails;

c. the prior art system appears to require and indeed, rely on, encryption to ensure that the program material which is communicated from a remote location is not intercepted for utilization in an unauthorized manner; and

d. it is unclear whether the system can accommodate and react appropriately to the situation where the program, once registered, is transferred in its entirety from one platform to another so as to avoid the requirement for payment of a further registration fee.

U.S. Pat. No. 4,796,220, assigned to Pride Software Development Corporation, discloses a system for unique recognition of a platform on which licensed software is to be executed. However, U.S. Pat. No. 4,796,220 does not contemplate or disclose utilization of information which is unique to the user or intended licensee as part of the registration process which is to be distinguished from identification of the platform upon which the software is proposed to be run.

U.S. Pat. No. 4,688,169 to Joshi broadly discloses the same principles as U.S. Pat. No. 4,796,220 in that it discloses a computer software security system which relies for its security on a "machine identification code unique to the machine" upon which the software to be protected is to be run. Again, the disclosure is limited to identification of the platform and there is no suggestion or contemplation of linking platform identification with unique user identification.

Also this arrangement does not allow the flexibility of transfer of copies of the program from platform to platform which can be run in a demonstration mode.

It is an object of the present invention to address or reduce the above-mentioned disadvantages.

Definitions

Throughout this specification the term "software" is to be interpreted broadly so as to include all forms of digital data which are executable on a platform (as to be later defined). The digital data comprising the software can, for example, be code comprising a word processing program adapted to run on a PC or the like. The software can also, for example, be digital data stored on a CD ROM adapted for playback as music on a CD ROM audio drive. The digital data can be displayable information or information which is otherwise usable by a licensed user.

Throughout this specification the term "platform" denotes an environment to be associated with a computing device such as a microprocessor or other data processing device which permits execution of the digital data (to which reference has previously been made in relation to the term "software") whereby the computer can perform functions on input and output devices associated therewith.

In some circumstances, the "software" or digital data may itself be the operating system environment. Typically, but by no means exclusively, examples of operating system environments include the MicroSoft DOS operating system, the IBM OS/2 operating system or the Macintosh System 7 environment. In the degenerate case of microcontrollers operating from ROM, the operating system environment may be the microcode of the microcontroller which enables the microcontroller to execute machine code.

In this specification, "use mode" refers to use of the digital data or software by its execution on a platform so as to fulfill the seller's/licensor's obligations in relation to the sale or license of the right to execute the digital data or software in the use mode. The use mode is to be distinguished from what might generally be termed unlicensed modes of operation (which is not to say unauthorized modes of operation) as typified by the demonstration modes later described in this specification.

SUMMARY OF THE INVENTION

In broad terms, the system according to the invention is designed and adapted to allow digital data or software to run in a use mode on a platform if and only if an appropriate licensing procedure has been followed. In particular forms, the system includes means for detecting when parts of the platform on which the digital data has been loaded has changed in part or in entirety as compared with the platform parameters when the software or digital data to be protected was for example last booted or run or validly registered.

The system relies on digital data or code which forms part of the digital data to be protected by the system. This portion of the digital data which preferably is integral to the digital data to be protected has been termed the "code portion" elsewhere in this specification. The code portion includes an algorithm adapted to generate a registration number which is unique to an intending licensee of the digital data based on

information supplied by the licensee which characterizes the licensee.

The algorithm in the code portion is duplicated at a remote location on a platform under the control of the licensor or its agents and communication between the intending licensee and the licensor or its agent is required so that a matching registration number can be generated at the remote location for subsequent communication to the intending licensee as a permit to licensed operation of the digital data in a use mode.

Preferably, the code portion is integral with the digital data and can be identical for all copies of the digital data. It is the algorithm embedded within the code portion (and which is duplicated at the remote location) which provides a registration number which can be "unique" if the information provided by the intending licensee upon which the algorithm relies when executed upon the platform is itself "unique."

In any event, in particular preferred forms, a serial number (see further on) is included in the registration number generation algorithm which introduces an additional level of uniqueness into the registration number calculation process.

Accordingly, in one broad form of the invention there is provided a system for licensing use of digital data in a use mode, the digital data executable on a platform, the system including local licensee unique ID generating means and remote licensee unique ID generating means, the system further including mode switching means operable on the platform which permits use of the digital data in the use mode on the platform only if a licensee unique ID generated by the local licensee unique ID generating means has matched a licensee unique ID generated by the remote licensee unique ID generating means.

Preferably, the system further includes platform unique ID generating means, wherein the mode switching means will permit the digital data to run in the use mode in subsequent execution of the digital data on the platform only if the platform unique ID has not changed.

Preferably, the mode switching means permits operation of the digital data in the use mode in subsequent execution of the digital data only if the licensee unique ID generated by the local licensee unique ID generating means has not changed.

Preferably, the mode switching means includes part of the digital data.

Preferably, the remote licensee unique ID generating means comprises software which includes the algorithm utilized by the local licensee unique ID generating means to produce the licensee unique ID.

Preferably, the information utilized by the local licensee unique ID generating means to produce the licensee unique ID comprises prospective licensee credit card number, date of birth and full name and address.

Preferably, the platform unique ID generating means forms part of the digital data.

Preferably, the platform unique ID generating means utilizes hard disk information and/or other computer hardware or firmware information to determine the platform unique ID.

Preferably, the platform comprises a computer operating system environment.

Preferably, the digital data comprises a software program adapted to run under the operating system environment.

In a further broad form of the invention, there is provided a security routine or registration means attachable to software to be protected, the registration means generating a security key from information input to the software which uniquely identifies an intended registered user of the software on a computer on which the software is to be installed.

Preferably, the security key is generated by a registration number algorithm.

Preferably, the registration number algorithm combines information entered by a prospective registered user unique to that user with a serial number generated from information provided by the environment in which the software to be protected is to run (e.g., system clock, last modify date, user name).

Preferably, the registration means is replicated at a registration authority and used for the purposes of checking by the registration authority that the information unique to the user is correctly entered at the time that the security key is generated by the registration means.

Preferably, the registration means checks at the time of boot of the software as to whether it is a first boot of the software to be protected or a subsequent boot. If a subsequent boot is detected, then environment and user details are compared to determine whether the program reverts to a demonstration mode and a new user registration procedure is to commence, or a full version run.

Preferably, the environment details comprise one or more of disc volume name, user name or computer, initialization date of hard disk, hardware identifier (e.g., ROM checksum) or other elements which are generally not user-configurable on the platform.

In a further broad form of the invention, there is provided a method of control of distribution of software, the method comprising providing mode-switching means associated with the software adapted to switch the software between a fully enabled mode and a partly enabled or demonstration mode; the method further comprising providing registration key generating means adapted to generate an enabling key which is a function of information unique to an intending user of the software; the mode-switching means switching the software into fully enabled mode only if an enabling key provided to the mode-switching means by the intending user at the time of registration of the software has matched identically with the registration key generated by the registration key generating means.

Preferably, the enabling key is communicated to the intending user at the time of registration of the software by a third party operating a duplicate copy of the registration key generating means.

In yet a further broad form of the invention, there is provided digital data incorporating registration code, the digital data executable on a platform; the registration code comprising a portion of the digital data executable on the platform so as to switch the digital data between a demonstration mode and a use mode.

Preferably, the registration code when executed on the platform provides local licensee unique ID generating means whereby the digital data can be switched from the demonstration mode to the use mode by execution of the registration code only if a licensee unique ID generated by the local licensee unique ID generating means has matched a licensee unique ID generated by remote licensee unique ID generating means.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described with reference to the accompanying drawings wherein:

FIG. 1 is a schematic diagram of the relationship and interaction between an intending registered user and a registration authority of software on media secured according to a first embodiment of the invention;

FIGS. 2*a*, 2*b* and 2*c* are segments of a flow chart of the procedure to be followed during registration of software by a user according to a first embodiment of the invention;

FIG. 3 is a flow chart of alternative boot processes according to a second embodiment of the invention;

FIG. 4 is a personal information dialogue box relating to the procedure of FIGS. 2*a*, 2*b*, 2*c* in accordance with a third embodiment;

FIG. 5 is a schematic diagram of a system according to a fourth embodiment of the invention;

FIG. 6 is an implementation of the fourth embodiment of FIG. 5 in relation to a CD ROM drive;

FIG. 7 is a logic flow chart in relation to the decoder box of FIG. 6;

FIG. 8 is a block diagram of a generalized system according to a fifth embodiment of the invention;

FIG. 9 is a block diagram indicating one particular example of generation of a registration number for the system of FIG. 8; and

FIG. 10 is a schematic diagram of a sixth embodiment comprising a particular example of the generalized system of FIG. 8.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

It is to be understood that, in its various embodiments, the present invention is for the protection of digital code/software by control of permission to use the digital code/software. A hardware platform and a remote registration station implemented at least partially by means of electronic hardware are required by the various embodiments.

The code/software to be protected requires at least some adaption to be usable with the invention in its various embodiments. The adaptation can be universal for all copies of the code/software to be protected.

First Embodiment

With reference to FIGS. 1 and 8, the system according to embodiments of the invention is designed and adapted to allow digital data 39 or software to run in a use mode on a platform 31 if and only if an appropriate licensing procedure has been followed. In particular forms, the system includes means for detecting when parts of the platform 31 on which the digital data 39 has been loaded has changed in part or in entirety as compared with the platform parameters when the software or digital data to be protected was, for example, last booted or run or validly registered.

The system relies on digital data or code 38 which forms part of the digital data to be protected by the system. This portion of the digital data, which preferably is integral to the digital data to be protected, has been termed the code portion 38 elsewhere in this specification. The code portion 38 includes an algorithm adapted to generate a registration number 66 or local licensee unique ID or registration key which characterizes the licensee. In this instance, the local licensee unique ID generator which generates the registration number comprises the execution of code 38 on platform 31.

The algorithm in the code portion is duplicated at a remote location on a platform 67 under the control of the licensor or its agents, and communication between the intending licensee and the licensor or its agent is required so that a matching registration number or enabling key can be generated at the remote location for subsequent communication to the intending licensee as a permit to licensed operation of the digital data 39 in a use mode.

Execution of the duplicated code portion on platform 67 comprises, in this instance, the remote licensee unique ID generating means.

Mode switching means can comprise execution of the code portion which additionally performs a comparison of the locally and remotely generated registration numbers.

Preferably, the code portion 38 is integral with the digital data and can be identical for all copies of the digital data. It is the algorithm embedded within the code portion (and which is duplicated at the remote location) which provides a registration number which can be "unique" if the information provided by the intending licensee upon which the algorithm relies when executed upon the platform is itself "unique".

In any event, in particular preferred forms, a serial number (see further on) is included in the registration number generation algorithm which introduces an additional level of uniqueness into the registration number calculation process.

With particular reference to FIG. 1, a program comprising digital data protected according to a first embodiment of the invention is supplied recorded on a magnetic disk 10.

Included as part of the software on that disk 10 is a registration and re-registration routine which executes whenever the program protected by the arrangement of the first embodiment "boots".

With reference to FIG. 1 and FIGS. 2*a*, 2*b* and 2*c*, the operation of the security routine will be described on the assumption that the program on the disk 10 protected by the registration routine has not been registered on the platform or is otherwise being loaded for the first time.

The prospective new user 11 inserts disk 10 into the user PC 12 so as to be read by PC 12.

As part of the software installation procedure, the registration routine is activated causing a series of dialogue boxes to appear on the display 13 of the user PC 12. Having checked to ensure that the software has not previously been registered on the PC 12, a dialogue box A (in FIG. 2*a*) is displayed which provides the user with a choice of either seeing a demonstration of the software (which typically has features such as save and/or print disabled) or alternatively an invitation to register ownership/licensee of the software (after which all features of the software are made available to the user).

If the register option is selected or if the user cancels the demonstration in favor of registration, then a contact dialogue box B (in FIG. 2*a*) is presented on the display 13 which provides a list (stored on disk 10 as part of the registration routine) which provides for example, names and contact numbers of the software publishing company together with other general product information.

Following the user's indication of agreement during display of license details (box B1) to proceed to register, the user can contact the registration center after filling out the registration dialogue box C as detailed below. After selecting "continue", the registration routine begins the first step in the generation of a security key which will be unique to the current copy of the software and to certain features of the environment in which it runs.

As shown in FIG. 2*b*, the first step in the generation of the security key comprises the generation of a serial number generated from the current time on the system and, in this example, the last modify date of the software and other information from the computer environment. The serial number is encrypted and rearranged and then presented as a number in the registration dialogue box on the display **13**.

The registration dialogue box C (in FIG. 2*b*) prompts the user for details unique to that user (including, for example, name, company, address, state, contact number) together with financial details for payment for the purpose of becoming a registered user of the software protected by the registration routine (for example Mastercard or corporate account number details). This information, unique to the user, is passed through a registration number algorithm **14** (represented symbolically in FIG. **1**) which generates a registration number or security key from the information unique to the user together with the serial number previously generated. The registration number or security key is not made available to the user of the PC **12** by the PC **12**.

An identical registration number algorithm **14** resides on the registration authority PC **15**. As an integral part of the registration procedure, the prospective new user **11** communicates the information unique to the user which was entered by the user on the user PC **12**, along with the serial number generated by the user's algorithm, to the registration authority **16**. The registration authority feeds this information into the registration authority PC **15** wherein the registration number algorithm **14** should produce an identical registration number or security key to that produced by the user PC **12** if the details communicated to the registration authority by the prospective new user **11** match with the details that have been entered on the user PC **12**. Optionally, the user can communicate the information to the registration authority electronically, e.g., by fax or modem or tone phone.

As a final stage in registration (refer to FIG. 2*d*), the registration authority **16** provides the registration number generated by the registration authority PC **15** to the user **11**. The user **11** enters the registration number into the user PC **12** where the registration routine checks to see whether the entered registration number matches the calculated registration number. If the two match, then a valid registration has taken place and access is provided by the registration routine to a full operating version of the software protected by the registration routine. If there is no match and a preference file (which stores the user details) does not exist then a dialogue box D (FIG. 2*c*) appears on the display **13** of user PC **12** providing the prospective new user **11** with the opportunity to check his/her details or switch to the demonstration version of the software protected by the registration routine.

Again, the registration authority PC **15** can provide to PC **12** the registration number which it generates by electronic means such as modem communication.

It will be evident that it is not obvious to the prospective new user **11** that the registration number which unlocks the full version of the software protected by the registration routine is, in fact, generated from an algorithm residing on the magnetic disk **10** and that it forms part of the software to which access is desired.

In this manner, the registration procedure outlined above ensures that exactly the same details entered by the prospective new user on his/her user PC **12** are those details recorded by the registration authority **16**. It will also be evident that the procedure does not require each magnetic disk **10** containing a copy of the software to be protected to have a unique registration number recorded on the disk at the time of distribution of the disk. Each copy has exactly the same registration number algorithm located upon it. A unique registration number or "security key" is generated only at the time of registration from the details supplied by the prospective new user **11**.

The registration routine behaves generally as follows where any copy of the protected software boots. In this situation, the registration routine checks at the time of boot to see what registration details are present for that particular copy of the software. If no details are present, then it is assumed that the PC is booting from a newly distributed magnetic disk and registration is to occur for the first time. The registration procedure in that case is that followed in respect of FIGS. 2*a*, 2*b* and 2*c*.

In the event that registration details are present, then the registration routine checks a number of parameters which are expected to be unique to the environment in which the software to be protected operates. In this embodiment, the parameters checked are hard disk volume name, user name, and computer name and user password and hard disc initialization date (not generally user configurable on the Apple Macintosh computer). The registration routine then checks these parameters against the corresponding details that it finds from the operating environment of the computer on which the software is running. If a designated combination of these details matches then it is assumed that a properly authorized and registered copy of the software is running and full access to the software is allowed.

In this manner, it is quite in order for users to provide other users with copies of the software protected by the security routine. The security routine attached to the software to be protected determines from the environment in which it operates whether an additional registration fee is required. If it is determined by the registration routine that this is the case, then the registration routine has the capability to provide a fresh registration number as part of an authorized registration procedure pending which the protected software reverts to demonstration mode.

Second Embodiment

(Auto re-registration)

According to a second embodiment, a more sophisticated procedure suitable for checking at first boot and at subsequent boot is shown in flowchart form in FIG. 3.

This procedure incorporates redundancy to cope with situations where the key file containing the information from which the current use has been authorized may have been deleted or does not exist on a subsequent boot.

The distinction as against the first embodiment is that a "key file" is created at the time of registration of the software and a duplicate key file is also created at the same time. The duplicate key file is arranged to be stored on the computer at a location separate from the program to be protected. In the case of the Apple Macintosh computer the duplicate key file can be stored in the "system" folder.

Both the key file (stored with the software) and the duplicate key file are encrypted and both contain identical information. The information contained comprises:

1. The user registration details including the serial number,
2. The environment details of the computer, and
3. Details of the application protected by the security routine for which registration is to be or has been obtained.

With reference to FIG. 3, whenever the protected application boots, a check is made by the registration routine to

determine whether registration details exist in the key file of the protected application. If they do, a comparison is made by the registration routine between what is stored in the key file and the environment to determine whether a change has taken place to the environment as compared with what is stored in the key file. If no change is detected, then the protected application is permitted to run normally.

If there are no registration details present in the key file or if the above-referenced comparison between the key file contents and the application does not show a match, then the re-registration routine of FIG. 3 looks for the existence of a duplicate key file within the environment. If a duplicate key file exists, then the information contained within that duplicate key file is copied to the application key file and comparisons as previously described as between the key file details and the environment and application are made. If the comparison is positive, then the protected application is allowed to run normally. If the comparison proves negative, then the protected application is permitted to run by the registration routine in demonstration mode only. If a duplicate key file is found not to exist at all and the internal key file, if present, brings a negative result, then the protected application is allowed to run in demonstration mode only.

This arrangement provides improved durability for the registration routine in the sense that it is less likely that the protected application will be caused to run in demonstration mode for incorrect reasons.

Third Embodiment

Tracking System

With reference to FIG. 4, a modified form of the dialogue box C of FIG. 2*b* is shown which includes provision for entry of "your user number" in box 21.

At the time a prospective new user enters his/her details into the other boxes comprising the dialogue box C, there is an option for the user to enter a user number into box 21. The user number is provided by the registration authority 16 as a number unique to that particular registered user. If the box 21 has the user number details inserted into it, then the registration routine, When the next copy of the protected application is made, will transfer the user number details from box 21 to the "last user number" box 22. A similar transfer will take place when next a copy is made of the protected application if and only if the person wishing to register the next copy enters their user number details in box 21. If they do not, then the last user number details in box 22 remain as before. In this manner, a tracking system is available to the registration authority in the form of a tree where any given copy is identified by its ancestry based on current and previous user number as entered into boxes 21 and 22.

Self-Serialization

In a particular embodiment, a process termed "self-serialization" can be utilized to produce the serial number 50 which is displayable to the user/licensee as illustrated in FIG. 4.

The serial number 50 is disguised by use of a random or pseudorandom number input to the algorithm which generates the serial number at the time of first boot of the software as part of the initial registration procedure. For example, the serial number, when generated by the self-serialization process, can be generated by a random number routine forming part of the registration software or it can be generated by the registration software with reference to data which is available in a widely varying fashion on the platform on which the software is located—for example, a time reference on the platform. The serial number 50 generated by the self-serialization process can be a required input to the registration algorithm from which the registration number is generated. Clearly, the serial number 50, as determined and displayed to the user, will then be required to be communicated to the registration authority for input to the registration authority's registration number generating algorithm.

It will be observed that a serial number 50 generated in this manner is likely to be displayed as a different number on each platform on which the software to be protected is to be run and comprises a randomized input to the registration algorithm which is determined and determinable only at the time of registration.

Fifth Embodiment

With reference to FIG. 5, there is shown in schematic form a microprocessor 30 adapted to operate under an operating system or upon a platform 31 such as, for example, MicroSoft DOS or Macintosh System 7. The platform 31 allows relatively high level commands to be used to cause the microprocessor 30 to interact with input/output devices such as keyboard 32, monitor 33, loudspeaker 34, memory 35 and magnetic or CD ROM disk 36.

By way of example a word processing program comprising a length of code or digital data 37 has been copied onto disk 36.

The digital data 37 includes registration code portion 38 and use code portion 39.

The digital data 37 is arranged in such a way that when microprocessor 30 seeks to first execute the digital data 37 by way of operating system or platform 31 the digital data comprising the registration code portion 38 is caused to execute first in a manner previously described in reference to the first embodiment of the invention. The execution of the digital data comprising the registration code portion 38 in conjunction with the operating system or platform 31 comprises a mode switcher which will permit the microprocessor 30 to execute the use code portion 39 of digital data 37 only in a demonstration mode unless and until registration involving reference to an external registration authority is first completed successfully. This registration procedure is as previously described with reference to the first embodiment.

The digital data 37 can comprise, for example, a word processing program such as Wordperfect 6.0 available from Wordperfect Corporation. The registration code portion 38 is integral with the digital data 37 comprising the word processing program. The registration code portion 38 includes the algorithm for calculation of the registration number as previously described in respect of other embodiments of the invention.

It will be appreciated that the registration code portion 38 effectively forms simply a part of the software or digital data 37 to be protected/registered and that the digital data 37 will be or can be identical for all copies of the word processing program produced. The registration code portion 38 allows a unique link to be made between the digital data 37 and an individual authorized or licensed to use the digital data 37 by way of initial execution of a copy of the digital data comprising registration code portion 38.

With reference to FIGS. 6 and 7, a specific realization of the fifth embodiment will be described.

With particular reference to FIG. 6, a decoder 51 is interposed in the datapath from the CD in CD player 52 and a digital-to-analog converter 53. The digital-to-analog con-

verter **53** is the device by which digitally encoded musical or video information residing on CD ROM **54** is converted to analog form suitable for playback on current mass produced television sets (video) or hi-fi sets (audio).

The decoder **51** comprises part of the platform upon which the digital data **37** is executed and includes means to interpret the code portion **38** of the digital data **37** whereby the registration system is implemented such that the digital data **37** and, more particularly, the use code portion **39** of that digital data **37** can be executed on the platform in a use mode only if the registration procedure to which reference has been made in respect of previous embodiments has been performed.

The registration code portion **38** can include a preview or demonstration related to a subset of the balance of the digital data on the CD **54** which can be executed by the platform without license.

The decoder **61** includes LCD display **55** and keypad **56** whereby the licensee can enter information via keypad **56** and receive information via the LCD display **55** for the purpose of the registration procedure.

In addition a smart card (SRAM) **57** is receivable by the decoder **81** for the purpose of customizing or amending operation of the decoder **51**.

With reference to FIG. **7**, the registration procedure following insertion of CD **54** into CD player **52** is as follows. The user operates the play control and decoder **51** reads from CD **54** code portion **38** of digital data **37** located thereon and executes this code so as to determine whether the digital data is already licensed for the platform. If not, a demonstration is communicated via digital-to-analog converter **63** whilst the user determines whether to register as a licensee of the digital data **37** in the manner indicated in the flowchart of FIG. **7**.

Sixth Embodiment

With reference to FIG. **8**, there is shown a block diagram of a system according to a further embodiment of the invention which is to be read in the context of the earlier generalized description in respect of FIG. **1**.

The system illustrated in FIG. **8** operates in the manner generally described in respect of previous embodiments and as generally outlined in the diagram. In the context of the block C illustrated in FIG. **4**, and with reference to FIG. **9**, the algorithm, which generates the unique user identification and which is resident both as the registration code portion **38** in digital data **37** integrally bound to use code portion **39** for execution on local platform **31** and also as remote algorithm **61**, is attached to registration database program **62** for execution on the remote platform **63**.

The algorithm, in this embodiment, combines by addition the serial number **50** with the software product name **64** and customer information **65** and previous user identification **22** to provide registration number **66**.

As discussed earlier, all of the items to be summed, namely items **50**, **64**, **65** and **22** must be communicated to the remote licensee unique ID generator **67** by the intending licensee whereby algorithm **51** causes the production of a registration number **66** which matches identically with the locally produced registration number. When mode switcher **68** verifies the match, then the mode switcher **68** allows execution on platform **31** of the full user program **39**.

Prior to allowing execution of the full program, mode switcher **68** will also check whether platform ID **69** has changed as provided to it by platform unique ID generator **70**.

In this embodiment, serial number **50** is comprised of two components, namely system information **71** and a variable key portion **72**. The variable key portion **72** provides the characteristic of self serialization described earlier in the specification and, in this embodiment, is generated at the time of registration on platform **31** by reference to a variable platform parameter, in this case reference to system time information, although other parameters which are variable can be utilized in other embodiments.

System information **71** can include information which identifies the hardware comprising the platform **31** on which the user program **39** is to be executed such as, for example, CPU number (where available), or unique parameters associated with the firmware in use. The system information, optionally, can further include system configuration information such as amount of memory, type of processor etc.

It will be noted, therefore, that serial number **50** will appear to an intending licensee when it appears on screen as per box C in FIG. **4** as an apparently random variable having no obvious link to the platform **31** or the user program **39**.

However, when the serial number **50** is communicated to the remote licensee unique ID generator **67** a secondary algorithm complementary to the algorithm which generated the serial number including variable key portion **72** and system information **71** is able to "decode" or otherwise strip away the variable key portion **72** so as to make use of the system information **71** if allowable and desirable in the circumstances.

Whether the system information **71** is utilized or not, the serial number **50** generated in this manner provides an input to the algorithm which generates registration number **66** which presents as an apparently variable parameter thereby rendering "cracking" of the software registration system more difficult and unlikely.

Seventh Embodiment

The schematic diagram of FIG. **10** illustrates a substantially hardware implementation of the invention applicable, for example, for implementation of the CD arrangement of FIG. **6** or the more generalized arrangement of FIGS. **8** and **9**.

In this embodiment, a prospective user **80** of digital code **81** on media **82** by its execution on platform **83** firstly inserts the media **82** into an appropriate digital code reading device within platform **83** (e.g., a floppy disk drive or a CD ROM drive).

Customer information C is provided by user **80** both direct to local encoder/decoder **84** and also to local adder or summer **85**.

Additionally, product information P derived from media **82** (typically via platform **83**) or else via the intermediary of the user (signified by the small man symbol) is provided to encoder/decoder **84** and to summer **85**.

Finally, a serial number S derived from platform **83** is supplied either directly or via the intermediary of user **80** to encoder/decoder **84** and to summer **85**.

Summer **85** acts as a local licensee unique ID generating means by combining, by addition, customer information C, product information P and serial number S in order to provide a local licensee unique ID here designated Y.

Encoder/decoder **84** transmits the serial number S, the customer information C and the product information P via

modems **86, 87** over the public switched telephone network to a remote encoder/decoder **88** which, in turn, supplies signals S, C and P to the inputs of remote summer **89**. Remote summer **89** combines these signals by addition (thereby acting as a remote license unique ID generating means) so as to provide a summed output, here termed X, which represents a licensee unique ID or enabling key which should match identically with the local licensee unique ID or registration key or registration number Y if inputs S, C and P to summers **85** and **89** are identical.

The licensee unique ID termed X is transmitted back via encoder/decoders and modems **84, 86, 87, 88** to comparator **90** which outputs a high signal if X equals Y. This condition corresponds to the local licensee unique ID matching with the licensee unique ID generated at the remote location by the remote licensee unique ID generating means generally comprising summer **89**.

Digital code **81** on media **82** comprises code identified as a demonstration portion D together with code identified as a use portion U. There may be other kinds of code designated O as well.

Code **81** is executed on platform **83** (for example, a microprocessor or a substantially hardware based, dedicated playback device such as a CD drive) with the code being passed through a mode switcher comprising first gate **91** and second gate **92** together with relay **93**.

First gate **91** energizes relay **93** so as to permit execution of code of type D but not code of any other type such as of type U.

Second gate **92** permits execution of any kind of code by closure of relay **93** provided only that the output of comparator **90** is high (which is to say that X equals Y or that the local licensee unique ID matches with the licensee unique ID generated by the remote licensee unique ID generating means comprising summer **89**).

Comparator **90** together with gates **91, 92** and relay **93** comprise one particular form of mode switcher or switching platform **83** of various kinds of code such as the code of types D and U.

Industrial Applicability

The aforementioned may be applied either in dedicated electronic hardware or by means of more generalized digital computation devices such as microprocessors and the like whereby digital code or software (which may incorporate at least part of the code which, when executed, acts as a licensee unique ID generator) is fully enabled only after following a specified licensing procedure.

The above describes only some embodiments of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope and spirit of the present invention.

What is claimed is:

1. A registration system for licensing execution of digital data in a use mode, said digital data executable on a platform, said system including local licensee unique ID generating means and remote licensee unique ID generating means, said system further including mode switching means operable on said platform which permits use of said digital data in said use mode on said platform only if a licensee unique ID first generated by said local licensee unique ID generating means has matched a licensee unique ID subsequently generated by said remote licensee unique ID generating means; and wherein said remote licensee unique ID generating means comprises software executed on a platform which includes the algorithm utilized by said local licensee unique ID generating means to produce said licensee unique ID.

2. The system of claim **1**, wherein said local licensee unique ID generating means generates said local licensee unique ID by execution of a registration algorithm which combines information in accordance with said algorithm, said information uniquely descriptive of an intending licensee of said digital data to be executed in said use mode.

3. The system of claim **2**, wherein said mode switching means permits operation of said digital data in said use mode in subsequent execution of said digital data only if said licensee unique ID generated by said local licensee unique ID generating means has not changed.

4. The system of claim **3**, wherein said local licensee unique ID generating means comprises part of said digital data when executed on said platform.

5. The system of claim **4**, wherein said mode switching means comprises part of said digital data when executed on said platform.

6. The system of claim **5**, wherein the information utilized by said local licensee unique ID generating means to produce said licensee unique ID comprises prospective licensee details including at least one of payment details, contact details and name.

7. The system of claim **1**, said system further including platform unique ID generating means, wherein said mode switching means will permit said digital data to run in said use mode in subsequent execution of said digital data on said platform only if said platform unique ID has not changed.

8. The system of claim **7**, wherein said platform unique ID generating means comprises part of said digital data when executed on said platform.

9. The system of claim **8**, wherein said platform unique ID generating means utilizes hard disc or other platform information to determine said platform unique ID.

10. The system of claim **1**, wherein said platform comprises a computer operating system environment.

11. The system of claim **10**, wherein said digital data comprises a software program adapted to run under said operating system environment.

12. A registration system attachable to software to be protected, said registration system generating a security key from information input to said software which uniquely identifies an intended registered user of said software on a computer on which said software is to be installed; and wherein said registration system is replicated at a registration authority and used for the purposes of checking by the registration authority that the information unique to the user is correctly entered at the time that the security key is generated by the registration system.

13. The registration system of claim **12**, wherein said security key is generated by a registration number algorithm.

14. The registration system of claim **13**, wherein said registration number algorithm combines information entered by a prospective registered user unique to that user with a serial number generated from information provided by the environment in which the software to be protected is to run.

15. The registration system of claim **12**, wherein said registration system checks at the time of boot of said software as to whether it is a first boot of the software to be protected or a subsequent boot, and, if a subsequent boot is detected, then environment and user details are compared to determine whether the program reverts to a demonstration mode and a new user registration procedure is to commence or a full version run.

16. The registration system of claim **15**, wherein said environment details comprise at least one element which is not user-configurable on the platform.

17. A method of control of distribution of software, said method comprising providing mode-switching means associated with said software adapted to switch said software between a fully enabled mode and a partly enabled or demonstration mode, said method further comprising providing registration key generating means adapted to generate a registration key which is a function of information unique to an intending user of the software; said mode-switching means switching said software into fully enabled mode only if an enabling key provided to said mode-switching means by said intending user at the time of registration of said software has matched identically with said registration key; and wherein said enabling key is communicated to said intending user at the time of registration of said software; said enabling key generated by a third party means of operation of a duplicate copy of said registration key generating means.

18. The method of claim 17, wherein said registration key is also a function of the environment in which said software is installed.

19. A remote registration station incorporating remote licensee unique ID generating means, said station forming part of a registration system for licensing execution of digital data in a use mode, said digital data executable on a platform, said system including local licensee unique ID generating means, said system further including mode switching means operable on said platform which permits use of said digital data in said use mode on said platform only if a licensee unique ID generated by said local licensee unique ID generating means has matched a licensee unique ID generated by said remote licensee unique ID generating means; and wherein said remote licensee unique ID generating means comprises software executed on a platform which includes the algorithm utilized by said local licensee unique ID generating means to produce said licensee unique ID.

20. A method of registration of digital data so as to enable execution of said digital data in a use mode, said method comprising an intending licensee operating a registration system for licensing execution of digital data in a use mode, said digital data executable on a platform, said system including local licensee unique ID generating means and remote licensee unique ID generating means, said system further including mode switching means operable on said platform which permits use of said digital data in said use mode on said platform only if a licensee unique ID generated by said local licensee unique ID generating means has matched a licensee unique ID generated by said remote licensee unique ID generating means; and wherein said remote licensee unique ID generating means comprises software executed on a platform which includes the algorithm utilized by said local licensee unique ID generating means to produce said licensee unique ID.

* * * * *

EXHIBIT B

COPY

FILED

2008 MAY 30 PM 3:51

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

BY _____

Scott R. Miller (State Bar No. 112,656)
smiller@cblh.com
Keith D. Fraser (State Bar No. 216,279)
kfraser@cblh.com
CONNOLLY BOVE LODGE & HUTZ LLP
333 S. Grand Ave., Suite 2300
Los Angeles, CA 90071
Tel: (213) 787-2500
Fax: (213) 687-0498

Attorneys for Plaintiffs,
Uniloc Corporation Pty Limited, Uniloc USA, Inc. and Uniloc (Singapore) Private Limited

IN THE UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

UNILOC CORPORATION PTY LIMITED, an Australian Proprietary Limited Company, UNILOC USA, INC., a Rhode Island Corporation, and UNILOC (SINGAPORE) PRIVATE LIMITED, a Singapore Corporation

Plaintiffs,

v.

XTREAMLOK, PTY, an Australian Proprietary Limited Company; and SYMANTEC CORPORATION, a Delaware Corporation, and DOES 1 to 10,

Defendants.

Civil Action No. _____

CV08-03574 DSF (CTx)

COMPLAINT FOR PATENT INFRINGEMENT, BREACH OF CONTRACT and VIOLATION OF CAL. BUS. & PROF. CODE §§ 17200 *ET SEQ*

Demand for Jury Trial

Plaintiffs Uniloc USA, Inc., Uniloc Corporation Pty Limited, and Uniloc (Singapore) Private Limited (collectively "Uniloc") file this complaint against Defendants XtreamLok Pty Limited ("XtreamLok") and Symantec Corporation ("Symantec"), and allege as follows:

The Parties

1. Plaintiff Uniloc Corporation Pty Limited (hereinafter "Uniloc Australia") is a Proprietary Limited Company existing under the laws of Australia. Plaintiff Uniloc USA, Inc. (hereinafter "Uniloc USA") is a corporation existing under the laws of Rhode Island. Plaintiff Uniloc (Singapore) Private Limited (hereinafter "Uniloc Singapore") is a limited liability company existing under the laws of Singapore. Uniloc's global headquarters and principal place of business is within this judicial district at 3333 Michelson Drive, Suite 600, Irvine, California 92612.

2. On information and belief, Symantec Corporation (hereinafter "Symantec") is a Delaware corporation having a principal place of business at 20330 Stevens Creek Blvd., Cupertino, California 95014.

3. On information and belief, XtreamLok is a Proprietary Limited Company existing under the laws of Australia. On information and belief, XtreamLok is a wholly owned subsidiary of Symantec and/or Symantec is the successor in interest to the business and obligations of XtreamLok.

4. Plaintiffs are ignorant of the true names of the defendants sued as DOES 1 through 10 and such names are fictitious. Plaintiffs will amend their Complaint if and when the true names of such defendants are ascertained.

Jurisdiction and Venue

5. This is an action for patent infringement arising under Title 35 of the United States Code as hereinafter more fully appears. This Court has jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1332. This is also an action for related breach of contract and unfair business practices. This Court has supplemental jurisdiction thereover pursuant to 28 U.S. 1367(a).

6. Upon information and belief, Defendants do business in this district and have committed acts of patent infringement in this district. In addition, the contract between the parties complained of herein was negotiated, entered into and breached in this district. Moreover, the contract includes a forum selection clause which specifies this District for the resolution of all disputes. Venue is proper under 28 U.S.C. §§ 1391(b)(2) and 1400, and per the agreement of the parties.

Background

7. The allegations in paragraphs 1-6 are incorporated by reference, as if fully set forth herein.

8. Uniloc, *inter alia,* researches, develops, manufactures and sells technology security solutions, including solutions for securing software and other forms of media.

9. On February 6, 1996, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 5,490,216 ("the '216 Patent"). The '216 Patent is entitled "System for Software Registration." A true and correct copy of the '216 Patent is attached hereto as Exhibit A.

10. The '216 Patent is generally directed to systems and methods for securely registering software and other digital media to prevent software piracy. Uniloc owns all rights, title, and interest in the '216 Patent.

11. On or about September 10, 2002, Uniloc entered into a Patent License Agreement with XtreamLok. The Patent License Agreement granted XtreamLok a non-exclusive license to use and sell the inventions described in the '216 Patent in limited territories. A true and correct copy of the Patent License Agreement is attached hereto as Exhibit B.

12. Pursuant to the terms of the Patent License Agreement, XtreamLok was required to pay to Uniloc a royalty based on all revenues received by XtreamLok for its sale of any of its products under the '216 Patent ("Licensed Products"). In addition, the contract requires XtreamLok to provide information and reports, pay a guaranteed minimum annual royalty as an advance against any royalties due during that same annual period ("Guaranteed Minimum

Royalty"), permit Uniloc access to records necessary to permit an audit of the royalties as paid and to submit to Uniloc samples of all Licensed Products.

13. On or after the effective date of the License Agreement, XtreamLok sold Licensed Products to Symantec.

14. Symantec thereafter made payments to XtreamLok for its use of Uniloc's Licensed Products. On information and belief, Symantec's royalty payments to XtreamLok far exceeded the amounts reported to Uniloc under the License Agreement and/or were arranged so as to artificially minimize such amounts in an effort to wrongfully reduce the royalties payable to Uniloc under the License Agreement. On information and belief, Symantec continued to make payments to XtreamLok for its use of Uniloc's Licensed Products in amounts in excess of the amounts reported to Uniloc under the License Agreement, or has sought to artificially minimize the reporting of such amounts in an effort to wrongfully reduce the royalties payable to Uniloc under the License Agreement.

15. XtreamLok has tendered to Uniloc, and Uniloc has rejected, the Guaranteed Minimum Royalty under the Patent License Agreement. Uniloc is informed and believes that such amounts understate the true amounts on which royalties are due to Uniloc under the License Agreement.

16. On information and belief, in or about May 2005, Symantec purchased XtreamLok. Thereafter, and continuing to the present, Symantec has

tendered to Uniloc, and Uniloc has rejected, the Guaranteed Minimum Royalty to Uniloc under the Patent License Agreement. Uniloc is informed and believes that such amounts understate the true amounts on which royalties are due to Uniloc under the License Agreement.

17. Uniloc has demanded information pursuant to the audit provisions of the License Agreement.

18. Defendants' actions have caused a failure of consideration of the Patent License Agreement and Uniloc has provided notice of such failure and its right to rescind the Patent License Agreement and/or Defendants' breach.

Count I – Breach of Written Contract

19. The allegations in paragraphs 1-18 above are incorporated by reference, as if fully set forth herein.

20. On or about September 10, 2002, Uniloc entered into the Patent License Agreement with XtreamLok.

21. XtreamLok breached the Patent License Agreement and/or caused a failure of consideration of the Patent License Agreement by, including, but not limited to, failing to pay the royalties due to Uniloc for XtreamLok's use and sale of the Licensed Products, by failing to provide samples of the Licensed Products to Uniloc for Uniloc's approval and by its failure to provide adequate information to Uniloc to allow Uniloc to properly audit the royalty reports made by XtreamLok and/or Symantec.

22. XtreamLok breached the Patent License Agreement and/or caused a failure of consideration of the Patent License Agreement by, *inter alia*, improperly categorizing the bulk of the payments received from Symantec for its use of Uniloc's Licensed Products as service fees instead of payments for use of Uniloc's licensed products and thus failing to properly account to and pay Uniloc the contracted royalty for the fees XtreamLok received from Symantec.

23. Symantec, as the successor in interest to XtreamLok and stands in the shoes of XtreamLok, has breached the Patent License Agreement and/or caused a failure of consideration of the Patent License Agreement by, including, but not limited to, failing to pay the royalties due to Uniloc for Symantec's use and sale of the Licensed Products and for failing to provide samples to Uniloc of the Licensed Products.

24. As a result of Defendants' breach of the Patent License Agreement, and/or as a result of the failure of consideration caused by the Defendants' actions, Uniloc has failed to receive the benefit of the bargain of the Patent License Agreement. As a result, Uniloc has suffered, and continues to suffer damages and irreparable injury, and Defendants and each of them have been unjustly enriched.

Count II – Infringement of U.S. Patent No. 5,490,216

25. The allegations in paragraphs 1-24 above are incorporated by reference, as if fully set forth herein.

26. XtreamLok's manufacture, use, offers to sell and sales of software security products, including, but not limited to, the Licensed Products, has directly infringed and continues to directly infringe one or more claims of the '216 Patent.

27. XtreamLok's actions have actively induced others to infringe one or more claims of the '216 Patent and/or has contributed to the infringement of one or more of the claims of the '216 Patent by XtreamLok's customers and/or their products.

28. On information and belief, Symantec manufactures, uses, offers to sell and sells software security products, including, but not limited to, Norton AntiVirus, using the technology licensed in the Patent License Agreement, including sales outside the Territory of the Patent License Agreement. As such, Symantec has directly infringed and continues to directly infringe one or more claims of the '216 Patent.

29. Symantec's actions have actively induced others to infringe one or more claims of the '216 Patent and/or has contributed to the infringement of one or more of the claims of the '216 Patent by Symantec's customers and/or their products.

Count III – Violation of Cal. Bus. & Prof. Code §§ 17200 *et seq*

30. The allegations in paragraphs 1-29 above are incorporated by reference, as if fully set forth herein.

31. Defendants' actions alleged above constitute unlawful, unfair or fraudulent business acts or practice in violation of the California Business & Professions Code §§ 17200 *et seq*.

Prayer for Relief

WHEREFORE, plaintiff Uniloc respectfully prays that the Court enter judgment in their favor and against Defendants as follows:

a. That XtreamLok be adjudged to have breached the Patent License Agreement;

b. That Symantec be adjudged to have breached the Patent License Agreement;

c. That the Patent License Agreement be rescinded;

d. That Uniloc be awarded all damages and/or quantum meruit and/or unjust enrichment to which it is entitled as a result of Defendants' breach of the Patent License Agreement and/or the failure of consideration.

e. That XtreamLok be adjudged to have directly infringed, induced others to infringe and/or contributed to the infringement of one or more claims of the '216 Patent;

f. That XtreamLok's infringement is found to have been willful, deliberate, and with actual knowledge of the '216 patent;

g. That Symantec be adjudged to have directly infringed, induced others to infringe and/or contributed to the infringement of one or more claims of the '216 Patent;

h. That Symantec's infringement is found to have been willful, deliberate, and with actual knowledge of the '216 patent;

i. That Uniloc be awarded all damages to which it is entitled under 35 U.S.C. §284;

j. That such damages be trebled pursuant to 35 U.S.C. § 284;

k. That the Court enter a preliminary and permanent injunction barring Defendants, their officers, agents, servants, employees and attorneys, alter-egos and their successors and assigns, as well as those persons in active concert or participation with them who receive actual notice of the judgment, from infringing, actively inducing the infringement of and/or contributing to the infringement of any claim of the '216 Patent, including, but not limited to making, importing, using, offering for sale, or selling any devices or systems that infringe, or using processes that infringe the '216 Patent;

l. That the Court find that this is an exceptional case under 35 U.S.C. §285 entitling Uniloc to an award of its attorneys' fees;

m. That Uniloc be awarded its costs and interest; and

n. That Uniloc receive such other and further relief as the Court deems just and proper.

Respectfully Submitted,

Connolly Bove Lodge & Hutz LLP
Scott R. Miller
Keith D. Fraser

Dated: May 30, 2008.

By: _____
Scott R. Miller

Attorneys for Plaintiffs
Uniloc USA, Inc., Uniloc Corporation Pty Limited, and Uniloc (Singapore) Private Limited

Demand for Jury Trial

Pursuant to Fed. R. Civ. P. 38(b) and Local Rule 38-1, plaintiffs Uniloc USA, Inc., Uniloc Corporation Pty Limited, and Uniloc (Singapore) Private Limited hereby demand a trial by jury on all issues so triable.

Respectfully Submitted,

Connolly Bove Lodge & Hutz LLP
Scott R. Miller
Keith D. Fraser

Dated: May 30, 2008.

By: _____
Scott R. Miller

Attorneys for Plaintiffs
Uniloc USA, Inc., Uniloc Corporation Pty Limited, and Uniloc (Singapore) Private Limited

EXHIBIT C

Scott R. Milller (State Bar No. 112656)
smiller@cblh.com
Keith D. Fraser (State Bar No. 216279)
kfraser@cblh.com
CONNOLLY BOVE LODGE & HUTZ LLP
333 South Grand Avenue, Suite 2300
Los Angeles, California 90071
Telephone: (213) 787-2500; Fax: (213) 687-0498

Attorneys for Plaintiffs UNILOC CORPORATION PTY LIMITED, UNILOC USA, INC., and UNILOC (SINGAPORE) PRIVATE LIMITED.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, SOUTHERN DIVISION

UNILOC CORPORATION PTY LIMITED, an Australian Proprietary Limited Company, UNILOC USA, INC., a Rhode Island Corporation, and UNILOC (SINGAPORE) PRIVATE LIMITED, a Singapore Corporation,

Plaintiffs,

vs.

XTREAMLOK, PTY, an Australian Proprietary Limited Company; and SYMANTEC CORPORATION, a Delaware Corporation, and DOES 1 through 10, Inclusive,

Defendants.

Case No. **CV 08-03574 DOC (MLGx)**

STIPULATION TO STAY CASE PENDING ARBITRATION OF PLAINTIFFS' BREACH OF CONTRACT CAUSE OF ACTION

[Proposed] Order Staying Case Pending Arbitration lodged herewith]

Hearing Date: October 27, 2008
Time: 8:30 a.m.
Courtroom: 9D, Santa Ana
Judge: Hon. David O. Carter

WHEREAS on May 30, 2008, Plaintiffs (collectively referred to herein as "Uniloc") filed this instant action against Defendants XtreamLok, Pty. ("XtreamLok") and Symantec Corporation ("Symantec") and asserted claims against each Defendant for Breach of Contract, Patent Infringement, and Unfair Competition;

WHEREAS on October 2, 2008, Defendants filed a motion to compel arbitration of all of Uniloc's claims pursuant to an arbitration clause set forth in a License Agreement entered into between Uniloc and XtreamLok;

WHEREAS Uniloc filed an opposition to the motion contending that its Patent Infringement and Unfair Competition claims were not subject to the arbitration clause of the License Agreement;

WHEREAS the parties have agreed, pursuant to the terms of the License Agreement, that this Court may determine the scope of the arbitration clause of the License Agreement.

WHEREAS the parties now wish to resolve Defendants' motion to compel arbitration;

WHEREAS the parties have agreed to arbitrate Uniloc's Breach of Contract action pursuant to the terms of the License Agreement;

WHEREAS the parties have agreed that, because resolution of Uniloc's Breach of Contract action may have a material impact on the other claims raised in the Complaint, this matter should be stayed pending arbitration of Uniloc's Breach of Contract action, and that, once the arbitration of that claim is concluded, this

matter may be re-activated so that this Court may address any remaining claims for Patent Infringement and Unfair Competition;

WHEREAS the parties agree that, once the arbitration is concluded, this Court may determine what, if any, impact the decision in the arbitration has on the other claims raised in the Complaint, and this Stipulation is without prejudice to assertions by the parties as to the impact of the arbitration on the claims and issues not decided by the arbitrator, which may be determined by the Court upon completion of the arbitration, in accordance with applicable law; and

WHEREAS the parties agree that at the conclusion of the arbitration, this court will retain jurisdiction to decide Uniloc's claims for Patent Infringement and Unfair Competition to the extent that either party contends any claims or issues remain in accordance with applicable law;

WHEREFORE IT IS HEREBY AGREED AND STIPULATED that:

(1) Uniloc's Claims against Defendants for Breach of Contract are subject to the arbitration clause of the License Agreement, and shall be submitted to arbitration in accordance with the Uniloc/XtreamLok License Agreement and applicable law;

(2) This action shall be stayed pending the arbitration of Uniloc's Breach of Contract claims against Defendants; and

(3) This Court shall retain jurisdiction over Uniloc's Patent Infringement and Unfair Competition Claims, and shall re-activate the matter upon application of the

parties upon completion of the arbitration to allow the continuation of the action as to any claims and issues which either party may contend remain to be resolved in accordance with applicable law.

SO STIPULATED

Connolly Bove Lodge & Hutz LLP

Dated: October 21, 2008

By: */s/ Scott R. Miller*
Scott R. Miller
Attorneys for Plaintiffs

Dated: October 21, 2008

Latham & Watkins, LLP

By: */s/ Mark A. Flagel (w/permission)*
Mark A. Flagel
Attorneys for Defendants

EXHIBIT D

Scott R. Milller (State Bar No. 112656)
smiller@cblh.com
Keith D. Fraser (State Bar No. 216279)
kfraser@cblh.com
CONNOLLY BOVE LODGE & HUTZ LLP
333 South Grand Avenue, Suite 2300
Los Angeles, California 90071
Telephone: (213) 787-2500; Fax: (213) 687-0498

Attorneys for Plaintiffs UNILOC CORPORATION PTY LIMITED, UNILOC USA, INC., and UNILOC (SINGAPORE) PRIVATE LIMITED.

JS-6

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, SOUTHERN DIVISION

UNILOC CORPORATION PTY LIMITED, an Australian Proprietary Limited Company, UNILOC USA, INC., a Rhode Island Corporation, and UNILOC (SINGAPORE) PRIVATE LIMITED, a Singapore Corporation,

Plaintiffs,

vs.

XTREAMLOK, PTY, an Australian Proprietary Limited Company; and SYMANTEC CORPORATION, a Delaware Corporation, and DOES 1 through 10, Inclusive,

Defendants.

Case No. **CV 08-03574 DOC (MLGx)**

ORDER STAYING CASE PENDING ARBITRATION

[Stipulation to Stay Case Pending Arbitration of Plaintiffs' Breach of Contract Cause of Action filed concurrently herewith]

Hearing Date: October 27, 2008
Time: 8:30 a.m.
Courtroom: 9D, Santa Ana
Judge: Hon. David O. Carter

The Court, having considered Plaintiffs Uniloc Corporation Pty. Limited, Uniloc USA, Inc., and Uniloc (Singapore) Private Limited, and Defendants Xtreamlok, Pty. and Symantec Corporation's Stipulation to Stay the Case Pending Arbitration of Plaintiffs' Breach of Contract Cause of Action, as well as the papers on the issue previously submitted by the parties, and finding good cause,

IT IS ORDERED THAT:

(1) Uniloc's Claims against Defendants for Breach of Contract are subject to the arbitration clause of the License Agreement, and shall be submitted to arbitration in accordance with the Uniloc/XtreamLok License Agreement and applicable law;

(2) This action shall be stayed pending the arbitration of Uniloc's Breach of Contract claims against Defendants; and

(3) This Court shall retain jurisdiction over Uniloc's Patent Infringement and Unfair Competition Claims, and shall re-activate the matter upon application of the parties upon completion of the arbitration to allow the continuation of the action as to any claims and issues which either party may contend remain to be resolved in accordance with applicable law.

(4) The hearing currently set October 27, 2008 is now VACATED.

IT IS SO ORDERED.

Dated: October 22, 2008

David O. Carter

Honorable David O. Carter
U.S. District Court Judge

Submitted by:

Connolly Bove Lodge & Hutz LLP

By: */s/ Scott R. Miller*
Scott R. Miller
Attorneys for Plaintiffs
UNILOC CORPORATION PTY LIMITED,
UNILOC USA, INC., and UNILOC (SINGAPORE)
PRIVATE LIMITED

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

I (a) PLAINTIFFS (Check box if you are representing yourself ☐)
Symantec Corporation
Xtreamlok, Pty

DEFENDANTS
Uniloc USA, Inc.,
Uniloc (Singapore) Private Limited,
Uniloc Corporation Pty Limited

(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.)
Mark A. Flagel
355 South Grand Avenue, Los Angeles, California 90071-1560
Telephone: (213) 485-1234

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an X in one box only.)

☐ 1 U.S. Government Plaintiff
☑ 3 Federal Question (U.S. Government Not a Party)
☐ 2 U.S. Government Defendant
☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only
(Place an X in one box for plaintiff and one for defendant.)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated or Principal Place of Business in this State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated and Principal Place of Business in Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. ORIGIN (Place an X in one box only.)

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify): ☐ 6 Multi-District Litigation ☐ 7 Appeal to District Judge from Magistrate Judge

V. REQUESTED IN COMPLAINT: **JURY DEMAND:** ☑ Yes ☐ No (Check 'Yes' only if demanded in complaint.)

CLASS ACTION under F.R.C.P. 23: ☐ Yes ☑ No ☑ **MONEY DEMANDED IN COMPLAINT:** $ according to proof

VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)
28 U.S.C. § 2201 et seq., 35 U.S.C. § 1, et seq.; Declaratory Judgment of Invalidity and Non-Infringement; Moneys Paid to Defendants

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES
☐ 400 State Reapportionment
☐ 410 Antitrust
☐ 430 Banks and Banking
☐ 450 Commerce/ICC Rates/etc.
☐ 460 Deportation
☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 480 Consumer Credit
☐ 490 Cable/Sat TV
☐ 810 Selective Service
☐ 850 Securities/Commodities/ Exchange
☐ 875 Customer Challenge 12 USC 3410
☐ 890 Other Statutory Actions
☐ 891 Agricultural Act
☐ 892 Economic Stabilization Act
☐ 893 Environmental Matters
☐ 894 Energy Allocation Act
☐ 895 Freedom of Info. Act
☐ 900 Appeal of Fee Determination Under Equal Access to Justice
☐ 950 Constitutionality of State Statutes

CONTRACT
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loan (Excl. Veterans)
☐ 153 Recovery of Overpayment of Veteran's Benefits
☐ 160 Stockholders' Suits
☐ 190 Other Contract
☐ 195 Contract Product Liability
☐ 196 Franchise

REAL PROPERTY
☐ 210 Land Condemnation
☐ 220 Foreclosure
☐ 230 Rent Lease & Ejectment
☐ 240 Torts to Land
☐ 245 Tort Product Liability
☐ 290 All Other Real Property

TORTS
PERSONAL INJURY
☐ 310 Airplane
☐ 315 Airplane Product Liability
☐ 320 Assault, Libel & Slander
☐ 330 Fed. Employers' Liability
☐ 340 Marine
☐ 345 Marine Product Liability
☐ 350 Motor Vehicle
☐ 355 Motor Vehicle Product Liability
☐ 360 Other Personal Injury
☐ 362 Personal Injury-Med Malpractice
☐ 365 Personal Injury-Product Liability
☐ 368 Asbestos Personal Injury Product Liability

IMMIGRATION
☐ 462 Naturalization Application
☐ 463 Habeas Corpus-Alien Detainee
☐ 465 Other Immigration Actions

TORTS
PERSONAL PROPERTY
☐ 370 Other Fraud
☐ 371 Truth in Lending
☐ 380 Other Personal Property Damage
☐ 385 Property Damage Product Liability

BANKRUPTCY
☐ 422 Appeal 28 USC 158
☐ 423 Withdrawal 28 USC 157

CIVIL RIGHTS
☐ 441 Voting
☐ 442 Employment
☐ 443 Housing/Accommodations
☐ 444 Welfare
☐ 445 American with Disabilities - Employment
☐ 446 American with Disabilities - Other
☐ 440 Other Civil Rights

PRISONER PETITIONS
☐ 510 Motions to Vacate Sentence Habeas Corpus
☐ 530 General
☐ 535 Death Penalty
☐ 540 Mandamus/ Other
☐ 550 Civil Rights
☐ 555 Prison Condition

FORFEITURE / PENALTY
☐ 610 Agriculture
☐ 620 Other Food & Drug
☐ 625 Drug Related Seizure of Property 21 USC 881
☐ 630 Liquor Laws
☐ 640 R.R. & Truck
☐ 650 Airline Regs
☐ 660 Occupational Safety /Health
☐ 690 Other

LABOR
☐ 710 Fair Labor Standards Act
☐ 720 Labor/Mgmt. Relations
☐ 730 Labor/Mgmt. Reporting & Disclosure Act
☐ 740 Railway Labor Act
☐ 790 Other Labor Litigation
☐ 791 Empl. Ret. Inc. Security Act

PROPERTY RIGHTS
☐ 820 Copyrights
☑ 830 Patent
☐ 840 Trademark

SOCIAL SECURITY
☐ 861 HIA (1395ff)
☐ 862 Black Lung (923)
☐ 863 DIWC/DIWW (405(g))
☐ 864 SSID Title XVI
☐ 865 RSI (405(g))

FEDERAL TAX SUITS
☐ 870 Taxes (U.S. Plaintiff or Defendant)
☐ 871 IRS-Third Party 26 USC 7609

SACV10-01483 JVS (MLGx)

FOR OFFICE USE ONLY: Case Number: _____.

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

VIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☑ No ☐ Yes
If yes, list case number(s): _____

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☐ No ☑ Yes
If yes, list case number(s): 2:08-cv-3574 DOC (MLGx)

Civil cases are deemed related if a previously filed case and the present case:
(Check all boxes that apply) ☑ A. Arise from the same or closely related transactions, happenings, or events; or
☑ B. Call for determination of the same or substantially related or similar questions of law and fact; or
☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
☑ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

(a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named plaintiff resides.
☐ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles County (Symantec Corporation)	Santa Clara County (Symantec Corporation) Australia (Xtreamlok, Pty)

(b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named defendant resides.
☐ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Orange County (Uniloc USA, Inc.)	Singapore (Uniloc (Singapore) Private Limited) Australia (Uniloc Corporation Pty Limited)

(c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** claim arose.
Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Orange County and Los Angeles County	

*** Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties**
Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER): _____ **Date** October 1, 2010

Notice to Counsel/Parties: The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge James V. Selna and the assigned discovery Magistrate Judge is Marc Goldman.

The case number on all documents filed with the Court should read as follows:

SACV10- 1483 JVS (MLGx)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

==========

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

[ ] **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

[X] **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

[ ] **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.